Endpoint Security

A state of transition

wanstor

Introduction

Endpoint security used to be a fairly mundane topic. The normal model used to be that the IT operations team would provision PCs with an approved image and then install Anti-Virus software on each system. The IT Operations team would then make periodic security updates (vulnerability scanning, patches, signature updates, etc.), but the endpoint security foundation was generally straightforward and easy to manage.

However in the last six months at Wanstor, we have seen an increase in the number of organisations increasing their focus on endpoint security and its associated people, processes, and technologies. This is largely down to mobility strategies starting to mature, BYOD becoming more common and mobile working the norm for many employees. Because of these market trends many businesses and not for profit organisations have had to increase their endpoint security budgets to cope with the changing working practices they are now facing.

The maturing of market trends have also meant many endpoint security vendors have had to change their strategies to cope with a transitioning end user workforce who want a stable office environment combined with a flexible work from anywhere approach.

At Wanstor we have seen the endpoint security strategy changing and predominantly being driven by the following factors in many organisations:

Cyber risks need to be addressed, especially around information security best practices

This is a clear indication that many IT security processes organisations have in place are not fit for a changing regulatory and mobile landscape.

Problems caused by the volume and diversity of devices

Addressing new risks associated with mobile endpoints should be a top endpoint security strategy requirement for all IT departments. This will only increase with the addition of more cloud, mobile, and Internet-of-Things (IoT) technologies

The need to address malware threats

Although it has been around for a long time many organisations are still struggling to get to grips with securing endpoints against malware threats. At Wanstor we do not find this overly surprising as the volume and sophistication of malware attacks has never been higher and the landscape is steadily becoming more dangerous.

Additionally the sophistication and efficiency of the cybercriminal underworld alongside the easy access that would-be criminals have to sophisticated malware tools are a combination organisations of all sizes need to take seriously.

At Wanstor we meet with 100's of customers on a regular basis and they are all saying the same thing – We are concerned about our ability to stop these malware threats and stay a step ahead of attackers.

While various industry research studies suggest endpoint security strategies are driven by the factors identified above, many businesses and not for profit organisations still struggle to address endpoint security vulnerabilities and threats with legacy processes and technologies as well.

Some of the most common things we see at Wanstor include:

Security teams spending too much time concentrating on attacks which are happening now and not planning for the future – As the threat landscape has evolved so has the pressure on endpoint security staff, systems and processes. In many organisations they only have 1 or possibly 2 trained IT security professionals. This means when an attack happens they have to spend a lot of time attending to high-priority issues. They do not have sufficient time for process improvement or strategic planning.

This challenge is something of a contradiction. Strategic improvements cannot and should not come at the expense of the security team failing to respond to high-priority issues, creating a quandary for many organizations: They know they need an endpoint security overhaul, but cannot afford to dedicate ample time at the expense of day-to-day security tactics. Effective endpoint tools must address this challenge by improving both the strategic and day-to-day position of the security team.

Organisations remain too focused/scared of regulatory compliance – At Wanstor we know it is a balance – IT security budgets vs regulatory compliance. However we have recently seen many businesses and not for profit organisations spending too much money/effort on becoming compliant within a changing regulatory landscape. Quite often this is because IT security teams have not worked with the business to properly define what the new regulations actually mean for the business and what the associated IT security spend should be. This often means IT security solutions are purchased ad-hoc and cost the organisation more money in the long run as they are purchased with a short term goal in mind rather than part of a wider security/regulatory plan.

At Wanstor we believe regulatory compliance should come as a result of strong security, and endpoint security cannot be achieved with a compliance-centric approach. For many IT teams this will mean a shift in thinking and closer working with other business departments such as the finance and legal teams.

Endpoint security has too many manual processes and controls – Endpoint security has undergone a major technical transition, but many organisations continue to rely on legacy products and processes to combat new challenges. It is often cheaper and easier for businesses and not for profit organisations to layer new products on top of legacy products as needs arise.

However the trade-off is IT security teams become more and more inefficient as they have several layers of security processes and tools they have to manage which can create a security operations nightmare.

Wanstor's Top Endpoint Security Challenges

- Security staff spending a significant amount of time attending to high priority issues leading to no time for process improvement or strategic planning
- Organisations too focused on meeting regulatory compliance requirements than addressing endpoint security risks with strong controls
- Endpoint security is based upon too many manual processes making it difficult for the security staff to keep up to date with relevant security tasks and new technology trends
- Organisations viewing endpoint security as a basic requirement and not giving it the time or resources it needs to protect users
- Lack of monitoring of endpoint activities proactively so it can be difficult to detect a security incident.
- Businesses and not for profit organisations not having access to the right vulnerability scanning and / or patch management tools so are always vulnerable to having an endpoint compromised by malware
- Lack of budget to purchase the right endpoint security products as IT teams unsure of how to develop the right business case for management teams to make decisions on

In summary, Wanstor's research of its own customers, and the changing mobility landscape identifies a situation where the principal endpoint security approach is not an adequate countermeasure for addressing the complexity and sophistication of modern IT security threats.

Wanstor's own customer and market research evidence strongly suggests that businesses and not for profit organisations at the moment do not view existing endpoint security strategies as viable for blocking sophisticated attacks.

As a result, many organisations need to supplement their existing endpoint security products with newer and more robust technologies that offer more functionality across incident detection, response, and remediation.

As a matter of course Wanstor believes all IT teams should take action now to review their endpoint security strategies and evaluate whether or not it is fit for purpose against business requirements. As a minimum the IT team should:

Investigate and test advanced anti-malware products – Organisations of all sizes should investigate and potentially acquire advanced anti-malware solutions. This is because normal solutions are no longer "good enough" to protect an organisation on their own. Instead IT teams need to recognise that all organisations are targets to hackers. In turn this means they should seek the strongest possible endpoint security solutions in order to deal with potential threats both now and in the future.

Continuous endpoint monitoring – The question has to be: – Does your IT team have the right network and security monitoring in place? If it doesn't how will you even know you are under attack or which endpoint devices are most vulnerable to attack? At Wanstor we always recommend appropriate network monitoring tools are purchased by the IT team. Quite often network monitoring and the ability to detect abnormal network traffic patterns early, help to prevent many security attacks before they become business critical.

Endpoint forensics – Endpoint forensic solutions can (when focused on actual need not cost) improve efficiency and effectiveness related to incident response, and reduce the time it takes for incident detection. Additionally by integrating endpoint data with network security analytics, it gives IT teams a more comprehensive and integrated view of security activities across networks and host systems.

Conclusion

In conclusion, endpoint security needs to change in most organisations to meet changing user needs and demands on IT. At the present time many organisations are struggling to hire the right staff, choose the right technologies, and respond to the many challenges of modern threats.

The scale and diversity of these challenges can appear overwhelming, but organisations that take the time to devise and execute solid, integrated endpoint security strategies can the right returns on their security investments and protect their organisations at the same time.

Wanstor believes that organisations who are seeking to overhaul their endpoint security should integrate their endpoint security technologies with their network-level and log monitoring in order to improve incident detection, prevention, and response, while also streamlining the work of their security operations team.

For more information about Wanstor's endpoint security services, click here

124-126 Borough High Street | London | SE1 1LB | info@wanstor.com

wanstor