HEAT® software

SOLUTION BRIEF

Operate with intelligence; make the service desk the first line of defence

In a world of 'zero day vulnerability' and 'advanced persistent threat', it is the service desk that can provide a vital first line of defence against industrial hackers.

"The biggest problem identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office … Virtually all organizations will evolve toward a more 'detect and respond' orientation from one that is focused on prevention."

Ponemon Institute: 2015 State of Endpoint Report: User Centric Risk

Security Beyond the Firewall

The frequency, size and level of sophistication of cyber-crime has evolved alongside advances in technology and changes in practice. Today's malware scans for unpatched machines and has abandoned operating systems in favour of 3rd party apps, 'malware's vehicle of choice'. Mix this with the widespread use of non-Windows and 3rd party apps and you have a fertile ecosystem for infection.

Gartner has identified four key trends impacting on the security landscape: the industrialisation of hacking; the influx of consumer technologies into the enterprise; the mobilisation of the workforce, and finally the decoupling of hardware and applications. Focusing on technology alone to address these trends is simply not enough; it's a business risk that requires enterprise – wide involvement.

For example, the leadership team need to understand that their HR department is just as important as their IT department when it comes to implementing a cyber security strategy. The Ponemon Institute's 2015 State of the Endpoint Report: User-Centric Risk suggests that the greatest risk to company assets comes from employees, so good screening and management of staff should therefore be a priority. Many organisations invest significantly on building strong fire walls, but don't necessarily monitor the development of potential threats against their business, nor the risks that can, and do, emanate from their own people.

Every employee is an entry point into your network and its concerning that employees are able to connect personal devices to their network unchecked due to non-existent or unenforced policies. Though many companies do not want to believe that their trusted employees would ever put their organisation at risk, the truth is that 75% of organisations report experiencing a data breach due to insiders, be it through negligence or malicious activity.

> "While it is positive news that companies are making the security of endpoints a higher priority, to win the war they need to recognize the criticality of minimizing employee negligence and investing in technologies that improve the ability to detect malicious attacks."
>
> Larry Ponomon, Chairman of the Ponomon Institute

Service Desk: The First Port of Call

So how do you mitigate insider risk? Simply put, the best security defence is knowledge, and the biggest thing any business can do to mitigate risk is to know exactly what is inside their network in order to identify strange behaviours and meaningful trends. Nobody is better positioned within the organisation to carry out this activity than the service desk as, when a user's PC is running slowly or a business application is frequently crashing, their first call will likely be to IT support in order to sort the issue out.

Taken in isolation these problems are relatively routine and easily dealt with. However, when they start happening simultaneously across a number of different users and devices it can act as an early warning system of a wider problem or even a potential cyber-attack. For example, in 2014 the US retailer Target suffered an incident when hackers generated $53.7 million by stealing credit card details, resulting in the CEO losing his job. There were many 'incidents' or 'signals' raised during the attack which, if resolved in a timely manner, could have minimised the damage.

If you take a close look at failures in security, the common factor appears to be a breakdown in change-control. If you don't know something has changed then you can't control it. The fact is that today you can't keep users from installing applications. So you need to know when compromised devices are plugged into the network, what social media and web-apps are being launched, and have a mechanism to stop it.

> "14% of executives surveyed admitted to lacking a strategy and being reactive when it came to information security"
>
> PWC: cybersecurity: The new business priority

Given access to the right tools the service desk offers a powerful first line of cyber defence. The proactive management of operating systems and application vulnerabilities with automated patching; endpoint protection to ensure only authorised applications run; policy-based enforcement of removable devices to control data in/out of endpoints; application control and intelligent white-listing for endpoint security are all pre-requisites to making this happen.

Ultimately, the net effect is having a service desk that is always truly on the front foot, one that is capable of moving from a heavily reactive approach, to a proactive one. Only then can you identify problems, as well as pre-empt certain problems before they impact the user.

A good service desk is cost-effective, improves workflow, and protects from debilitating, costly and embarrassing security breaches. It's all about visibility, insight and control. Critical to security it can secure access points, enable device freedom and create a resilient corporate infrastructure to enable holistic management of performance and security. And it also cuts IT operating costs and enables productivity.

In many ways controlling change is the key to 'defence grade security'. In 2014 it took a median of 205 days to detect an attack. The fact is that in a world of advanced persistent threat, everyone in the organisation needs to be taking responsibility for cyber security and the front line of defence is always the service desk. It provides visibility of the network and endpoints, insights into what is going on, and the capability to control what happens.

About HEAT Software…

HEAT Software is a truly powerful combination of industry leaders: FrontRange, the industry's sole provider of Hybrid Service Management (HSM) and Endpoint Management; and Lumension, the industry's leading Endpoint Security provider.

Only HEAT Software commands the intersection of HSM and Unified Endpoint Management (UEM), empowering IT, HR, Facilities, Customer Service and other enterprise functions to simplify and automate their business processes, manage and secure endpoints and proactively detect and protect against threats to business continuity.

HEAT is the only company in the world that manages services and endpoints securely across the same platform, on premise or in the cloud, via desktop or mobile applications.

HEAT's customers consistently achieve increased operational efficiency and greater system sustainability through optimised business processes, and efficiently managed and secured endpoints.

Tap into the world's most powerful fusion of truly flexible, scalable, secure HSM and UEM solutions.

Forged by HEAT.

HEAT Software
Email: marketinguk@heatsoftware.com
Website: www.heatsoftware.com