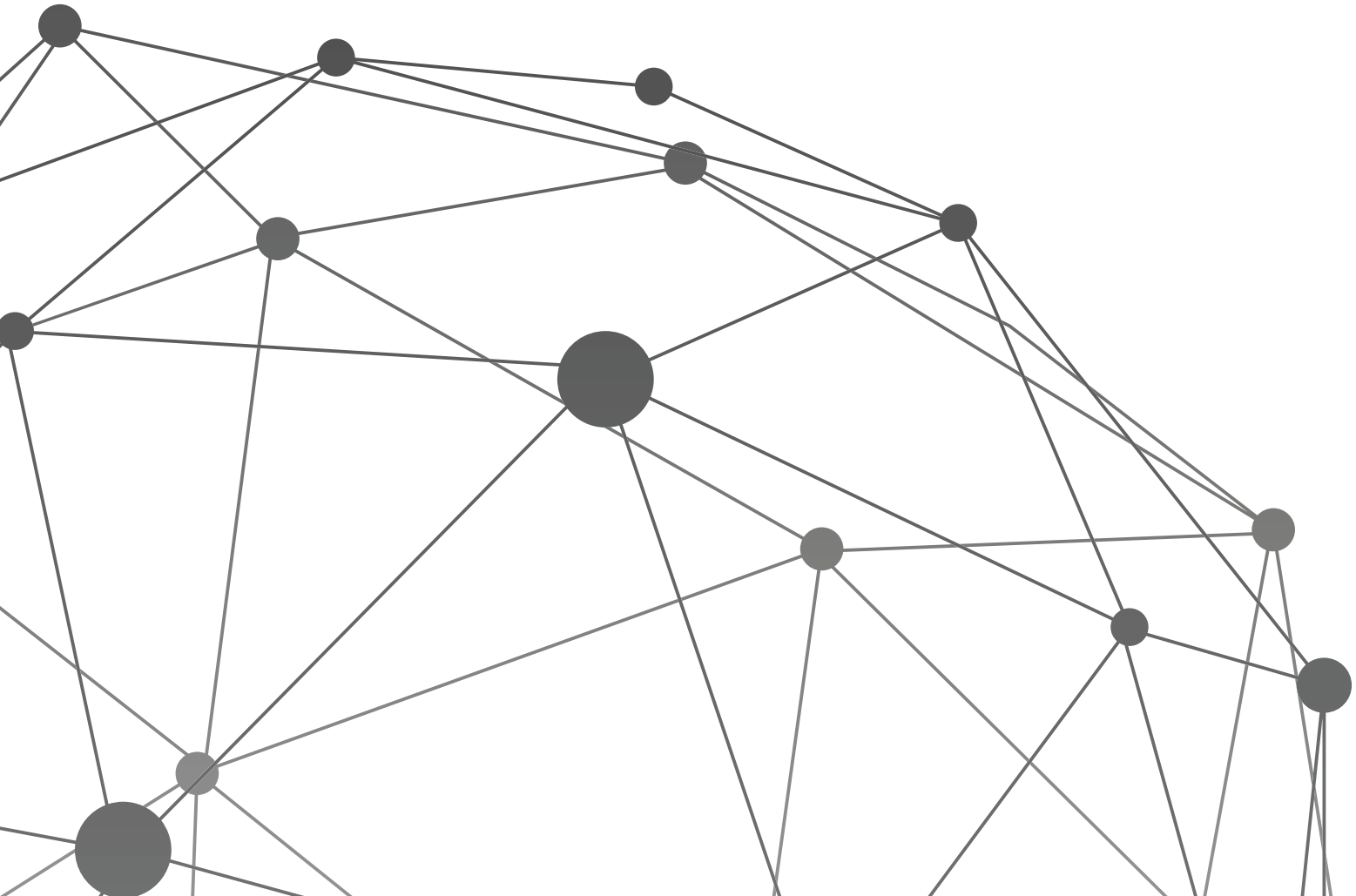
HEAT® software

Security Threat Landscape FAQ



What should companies be most worried about within the evolving security threat landscape?

There are millions of cyber-attacks taking place every day with a total cost to the global economy of up to $575 billion a year. Data breaches will carry on, however, given the effectiveness of malicious programmes like ransomware and recent events such as the Ashley Madison hack which proved devastating for business, 2016 seems likely to be the year we see an explosion in online extortion, be it for financial, political or moral reasons. Companies therefore need to make plans based on not if, but when, they will be attacked.

Companies must think like an attacker and act like a defender. 90% of business risk can be eliminated by proactively managing vulnerabilities. To do this successfully requires a multi-layered approach that monitors your endpoints. A 360 degree approach includes vulnerability and patch management, application control, hard drive and media encryption, device control and antivirus.

Does the biggest threat come from inside or outside the organisation's network?

It's not just cyber-attacks an organisation needs to be aware of. In terms of network security it is possible to lock everything down to prevent external hacks. However dealing with the 'enemy within' is much more difficult and equally as damaging.

Every employee is an entry point into your network and can introduce significant security risks be it by accident or malicious intent. For example this could be employees innocently clicking on an email link that they shouldn't open, downloading an unapproved app, losing removable devices, laptops or mobile phones or intentionally walking out of the office on their last walking day with valuable data on a USB. Employees are also accessing their network using their own personal devices, often unchecked due to non -existent or unenforced security policies.

Just like an operating system, people store, process and transfer information, so they should really be viewed in the same light when it comes to security.

Why is anti-virus alone not an effective corporate defence?

Almost every company runs anti-virus software as it's an important part of network defence, but the problem is, they're still getting infected with malware. Due to its blacklisting approach, anti-virus does a good job of stopping fast-spreading and widely known threats. However with the exponential growth in malware and the exploitation of application vulnerabilities, anti-virus software can't keep up and offers no protection against malware it is yet to be exposed to or zero-day vulnerabilities. What you need is more effective endpoint security which includes intelligent whitelisting as this provides greater protection, productivity and efficiency.

What are the biggest threats to organisations endpoints?

According to the Ponemon Institute, the primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies. This follows the increase in the number of personal devices now being connected to the network, increase in commercial cloud applications and the increase in mobile workforce.

Move towards a more 'detect and respond' orientation to counteract data breaches and increased vulnerabilities.

One of the biggest mistakes that companies make with their security measures is that too much emphasis is placed on prevention alone, when detection and response are just as, if not more important, If a hacker is already inside your network, you need to be able to immediately understand how they got in, what they have accessed and how you can remediate that threat, and that can only be achieved with a layered system of defences that provides you with real-time visibility.

Whose responsibility should security be within an organisation?

Cyber security is a shared responsibility and the HR department is just as important as the IT department and service desk when it comes to implementing an effective 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 by the HR team 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.

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.

How should organisations respond to upcoming legislation such as the EU GDPR?

The introduction of legislation such as the EU GDPR and German IT Security Act is encouraging but must be seen as the starting point for any company's security strategy rather than a tick box exercise that is forgotten once compliance is achieved. Legislation aims to bring organisations up to a minimum level of security but is purely reactive in the sense that it only consists of a sensible level of protection against known threats.

A combination of people, processes and technology is needed to put up a unified front against all external threats. This is where giving the IT, security or service desk teams the tools to keep track of all devices connected to the network can help create a culture in which everybody is aware of their responsibilities.

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 optimized 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