Intelligent security for high performance business

Today cybercrime and espionage operate like any other business.

They recruit the brightest talent, invest heavily in R&D and in expanding their global ‘distribution’ capabilities.
A new approach for a new era of cyber threats

Organizations today are more reliant than ever on information to achieve success. Information is, perhaps, your most precious business asset. And that’s why cyber criminals are spending millions developing extremely sophisticated attacks. It’s also why competitors and hacktivists will go to extraordinary lengths to acquire your intellectual property.

A quick glance at the news highlights the difficulties organizations of all types and sizes have in protecting their data. The challenge lies in the fact that information security is not one of your core activities – but it is for the cyber attacker!

Today cybercrime and espionage operate like any other business.

They recruit the brightest talent, invest heavily in R&D and in expanding their global ‘distribution’ capabilities. Cybercriminals can achieve their goals through Cybercrime-as-a-Service, a black market service that offers rapid access to pre-prepared, sophisticated malware and techniques, including ransomware and Advanced Persistent Threats (APTs).

How can organizations like yours hope to defend their critical data, operations and reputations against a sophisticated and motivated enemy?

Imagine the personnel and systems investments required just to keep up with detecting possible cyber attack incidents, let alone creating a proactive, intelligent, real-time defence.

Now is the time to look at a new approach to security delivered by a highly experienced partner.
The cyber threat landscape is in a constant state of flux. Cyber thieves and spies already possess tools that allow them to cost-effectively develop advanced attacks and accelerate the pace of innovation. Going forward, evasion techniques are likely to be deployed more often, helping the malware to avoid detection. Custom-developed attacks will also be deployed more readily in order to exploit unique vulnerabilities in an organizations systems.

The key to prevent cyber attacks

So what types of threat should any security strategy take into consideration? Clearly the threat landscape is constantly evolving, yet we can make some sound predictions about what the future may hold – and the following are likely to be in abundance:

**Email and SMS phishing**
Simple to attack, difficult to defend, easy to misuse.

**Ransomware**
Can be effective in the cloud, on mobile devices, anywhere. Difficult to prevent and even harder to defeat.

**Point-of-sale attacks**
POS terminals are already under attack and this will grow as payment types (mobile apps) expand.

**Insider threats**
Emanating from disgruntled employees, lapses in partners’ security or even data loss from misplaced or stolen employee devices.

**Mobile malware**
The proliferation of mobile devices makes mobile and BYOD an extremely rich attack surface.

**Non-Windows malware**
Driven by the after effects of the Shellshock vulnerability as attackers target vulnerable Unix and Linux devices.

**Internet of Things attacks**
Will increase in order to harvest the valuable data these connected devices gather. The attacks will likely increase in frequency, profitability and severity.

**Advanced Persistent Threats: Espionage & cyber warfare**
Such skirmishes will likely occur between nation states. Governments will increasingly use malicious software to monitor the activities of persons of interest and to organise targeted attacks. Cyber criminals and business rivals will also use sophisticated attacks to spy on commercial activities and steal intellectual property.

Despite the threats and in order to be competitive, your organization cannot lock down its systems and data. The free flow of information supports innovation, productivity, customer experience, back-office operations – almost everything your people do every minute of the day. An intelligence-based, context-aware approach to information security is the answer – but only one that will not add to IT’s operational or budget burden.

Its Security Information and Event Management technology, called McAfee Enterprise Security Manager (ESM) provides corporates and public sector organizations with the ability to capture, consolidate, correlate, assess, and prioritise security events for both third-party and Intel Security solutions in real-time.

What this creates is an intelligence-based approach to information security that is ideal for today’s high performance operational environment.

McAfee ESM can answer multiple queries about events and activity within your environment. It does this by analysing network activity including, for example, full database sessions, alongside other criteria such as user behaviour, device location and user roles, as well as the content within transmitted documents. By aligning this data to your particular risk profile, it will assess whether certain activities may be harmful or malicious. And it can do it in real-time, reducing time from detection to containment to mere milliseconds.

The technology also links into McAfee’s global threat database, McAfee Global Threat Intelligence, to correlate suspected events against known malware signatures.

McAfee’s unique Threat Intelligence Exchange technology distributes event information to connected security technologies such as next generation firewalls and intrusion prevention systems, creating a crucial framework for sharing security intelligence.

What makes McAfee ESM so powerful is that all this proactive monitoring is collated and presented through a single pane of glass, where event management is logged and reporting against some 240 data usage regulations is automated for you.

For maximum protection, McAfee ESM scales to your needs, supporting hundreds of thousands of events per second. As fantastic as this capability sounds, we can further enhance its capabilities.

Let’s discover how…
Atos High Performance Security: Transform your security

We selected Intel Security’s McAfee Enterprise Security Manager to power our powerful managed security service - Atos High Performance Security (AHPS).

AHPS delivers a holistic approach to information security, delivered through our Assess & Design, Transform and Operate philosophy. Thanks to more than 25 years of experience delivering security solutions to our enterprise customers, we will undertake the following activities in collaboration with you:

Assess & Design
Audits your security needs using industry best practice to evaluate your risk profile and information compliance obligations and to define the necessary controls. We will ensure we deploy the most appropriate solution for your particular needs.

Transform
Your security posture by engineering AHPS to deliver the protection and reporting your organizations requires. This may include activities such as proof of concept and solution testing.

Operate
your AHPS service for you from our state-of-the-art Security Operations Centers (SOC) around the world.

Peace of mind
achieved from the knowledge that your data is being monitored and protected 24/7 by a global network of expert security analysts. Your team will constantly monitor your environment, evaluate potential security vents and undertake first phase investigations in order to help block an attack.

Cost savings
derived through the significant economies of scale you would expect from a centralised, managed service. Could your organizations recruit the thousands of security personnel you can rely on from us?

Simplicity
we take care of every aspect of your service from end-to-end, so there are no third parties to manage and just one dedicated point of contact with whom to liaise.

Actionable security intelligence
as a renowned systems integrator we can help you make the absolute most of the security intelligence that our SIEM technology delivers. By integrating it into your endpoint protection technologies we can help you create a robust, continuous system of actionable security data to defend you against even the most sophisticated threats.

In practice, our service management methodology, illustrated below, creates a dynamic, intelligence-based feedback loop (see Figure 1). This means we can build a solution that understands and adapts to your changing business requirements, analyses your particular risk profile and monitors for abnormal behaviour so that we can respond to incidents in real-time. We also measure the effectiveness of your solution in relation to external threat intelligence and make the necessary ongoing adjustments that will keep your critical data and systems safe. By combining this methodology with unique capabilities AHPS delivers business advantages that are simply unbeatable. These include:

Understand

- Identify normal behaviour
- Define criticality of systems & data
- Define security metrics

Measure security posture

- Audit
- Monitor for abnormal behaviour
- Respond to the incident

Analyse

- Evaluate the risk (based on scenarios)
- Define controls (based on scenarios)

Build

- Implement architecture
- Enforce monitoring architecture technology
- Enforce security controls using technology
- Use adopted real time risk management technology

Figure 1

Figure 06

With all this in mind, we are stronger together...
In creating Atos High Performance Security, we tested many SIEM technologies, undertaking proof of concept tests, analysing results and determining innovation roadmaps. What sets us apart is that we have selected the very best solution in the market, McAfee Enterprise Security Manager. It is backed by the might of Intel and, we believe, offers you unmatched capabilities and a pathway to a robust, proactive, connected security posture.

Some of the world’s most prestigious organizations – our customers – would agree. They rely on Atos and Intel Security to jointly keep their critical information and systems secure so that they can be deployed for maximum business advantage.

In fact, because innovation lies at the core of our business strategy we are compelled to remain one step ahead of today’s threat actors. With this in mind, the Atos Scientific Community, our ‘creators of change’ are involved in anticipating shifts in the global threat landscape and developing actionable thought leadership on the subject along with new and disruptive solutions to the ongoing challenge of security.

With this support our customers will be empowered to safely take advantage of new technologies in order to reinvent their growth models and build a sustainable competitive advantage. This demonstrates our commitment to working in collaboration with all our customers, sharing operational learnings and key security insights that will help to mitigate the risk of cyber attacks ever being successful in their environment.

With over four billion people watching the 2012 Olympic Games, the London Olympic Games could afford zero security incidents. We achieved exactly that. And we did it again at Rio 2016.

The Atos SIEM platform received over 255 million syslog messages during the Olympics

From these raw messages 4.5 million significant events were identified

SIEM raised internal incidents for 5,324 of these events for SOC assessment

Of these internal incidents 686 were raised to venues as tickets

During the Olympic Games zero security incidents impacted live competition Atos

Discover how we can advance your security so that you can focus your on business success.

For more information, please contact us at security@atos.net or visit atos.net/security
About Atos

Atos SE (Sociétas Europaea) is a leader in digital services with pro forma annual revenue of circa €12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

Find out more about us
atos.net
ascent.atos.net

Let’s start a discussion together

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique McAfee Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world.

intelsecurity.com