



Security-as-a-Service: The Future of Security Management



Creative ITC

EVERY SINGLE ATTACK THAT AN ORGANISATION EXPERIENCES IS EITHER ON AN ENDPOINT OR HEADING THERE

65% of CEOs say their risk management approach is falling behind. In a new reality where security breaches come at a daily rate, we must move away from trying to achieve the impossible perfect protection and instead invest in detection and response. **Organizations should move their investments from 90% prevention and 10% detection and response to a 60/40 split.**

Peter Sondergaard

Senior VP and Global Head of Research
Gartner



Staying ahead in today's cyber landscape can be tough; especially if you've been relying on rigid, manual processes and siloed technologies. The security products you need are easy to buy, but not necessarily easy to manage. And organisations don't always have the internal resources or expertise.

Cloud-based security offers companies a way forward without on-premise devices. But, the challenge of managing security internally still remains. Creative's Security-as-a-Service approach is a new way to stay ahead, while also reducing burden on your IT teams.

Our fully managed, cloud-based approach provides access to powerful tools and real-time threat intelligence. So, you can instantly spot, react and stop threats in their tracks. All with the comfort of being managed by a team of world class security specialist engineers.

THE FUTURE OF SECURITY MANAGEMENT

Our Security-as-a-Service portfolio helps customers make their environments more agile, automated and interconnected. Security remains the number one concern for most CIOs and their IT departments. They're increasingly turning to Security-as-a-Service in order to strengthen protection and consolidate vendors.

That's because:

1. In the UK, a cybercrime or fraud is committed every four seconds
2. 40% of threats come from insiders
3. Every single attack starts from an endpoint or it's heading there
4. The average cost of a security breach is £2.6 million
5. 27% of organisations that use 50+ security vendors get breached within six months - compared to only 1% of organisations that use 5 vendors or less

OUR CREDENTIALS

Creative is an independent company: not reliant on protecting legacy platform revenues. This ensures our advice is impartial and draws on experience gained protecting some of the world's largest companies.

We cover security end-to-end: from data centres and networks, to desktops and remote workers.

With the best technical minds in the industry - including the highest level Cisco Security accreditations - we're passionate about helping our clients make their organisations more secure and cyber-resilient.

We have strategic partnerships with all the top security vendors, ensuring you'll always receive competitive pricing and quick answers.

Creative is also one of the few infrastructure partners to have its own Network and Security Operations Centre with industry leading systems for around-the-clock threat monitoring and analysis. So, we'll make sure security concerns won't keep you awake at night.



CYBER SECURITY WITH A DIFFERENCE

BUILT FOR SIMPLICITY AND SPEED

Choosing the right hardware and software is vital, but alone it's not enough. You may have the correct technology in place, but if you don't have effective processes and haven't trained your staff properly then you will just create more vulnerabilities.

We believe that effective cyber security has to be built on three pillars: **people, processes and technology**

Our experienced **people** ensure risks are identified, processes refined and technology implemented to industry best practice. The **processes** we create ensure full lifecycle management for each specific area of business risk. We only deploy best-in-class **technology** – onsite or in the cloud – in a layered approach for increased protection of your critical infrastructure. And we work closely with you to provide solutions to meet your needs.

A security engagement with Creative also goes further than the pick-and-mix of tools offered by point solution providers.

CONTINUOUS VISIBILITY, REMEDIATION AND REPORTING

Delivered as a tailored service

Key services include:



Remediation



Visibility



Reporting

Rather than deal with a multitude of dashboards, each pertaining to a particular cyber threat, you receive an integrated approach with a single, automated architecture.

WHAT DOES OUR SECURITY-AS-A-SERVICE INCLUDE?

1

SECURITY AUDIT

An onsite assessment of your existing security systems, software and processes mapped against industry best practices. The output is a detailed gap analysis, providing practical recommendations for improvement.

2

ENDPOINT AND DEVICE MANAGEMENT

The industry average time-to-detection is 100 days. Using our systems integration expertise we link a specific set of Cisco Security technologies to cut this to three hours or less.

3

SECURITY OPERATIONS CENTRE

Not every organisation wants to hire cyber experts and security analysts. Skilled specialists in our Security Operations Centre can help with the heavy lifting, acting on emerging threat intelligence and remotely monitoring and updating your IT security.

4

REPORTING AND ANALYSIS

Detailed dashboard reporting and analytics highlight key trends, changes to your threat landscape and security performance statistics. So you'll have all the information required to demonstrate effective controls to your management team.

5

VULNERABILITY AND PATCH MANAGEMENT

Ensuring continuous visibility is the first step in identifying vulnerabilities within your infrastructure. This allows risk to be assigned based on likelihood and impact, ensuring an appropriate response and audit trail to each threat, right through to successful remediation.

WHICH TOOLS DO WE USE AND WHY?

CISCO UMBRELLA

Boost front-line defences with the industry's first secure Internet gateway in the cloud, stopping malware before it reaches your endpoints and networks.

CISCO FIREPOWER NEXT-GENERATION FIREWALLS

Keep your users and networks safe by uncovering hidden threats with advanced malware and intrusion protection services.

CISCO ADVANCED MALWARE PROTECTION (AMP)

Prevent breaches and block malware by rapidly detecting, containing and isolating threats that have evaded your perimeter security.

EMAIL SECURITY

Combat ransomware, spoofing and phishing using advanced threat intelligence to protect inbound messages and sensitive outbound data.

CLOUDLOCK

Protect users of software-as-a-service and public cloud applications with cyber-security tools and analytics.

IDENTITY SERVICES ENGINE/ARUBA CLEARPASS

Unify and automate network access control, ensuring users and their devices are safe before using wired, wireless and remote connections.

AIRWATCH MOBILE DEVICE MANAGEMENT

Empower your mobile workforce with simple onboarding and greater uptime through robust policy enforcement and centralised management.

SOLARWINDS PATCH MANAGER

Improve security patching with pre-built packages, vulnerability dashboard management and compliance reports.

SOLARWINDS RISK INTELLIGENCE/QUALYS VULNERABILITY SCANNING

Spot at-risk data and simplify compliance with the latest remote scanning techniques and reporting tools.



Our Security Operations Centre wraps around all of the above tools.

All of our services are tailored to your exact requirements, with reliability and quality of service guaranteed by stringent service level agreements. You'll get access to our highly skilled security specialists, continuous visibility using advanced technology and proven processes to manage compliance.



BENEFITS INCLUDE:



Enhanced IT Security



Reduced business risk



Increased compliance



Additional time to innovate



Reduced staff costs

With the average industry time to detect a breach currently at 100 Days, at Creative we aim for a target of 3.5 hours or less.

Our financial packages roll people, processes and technology into one OpEx-based approach, structured on a per-user, per-month basis – providing you with a simple, predictable cost model for your entire security landscape.

By 2020 there will be between 1-2 million unfulfilled IT security jobs worldwide.

TODAY'S CHALLENGE AND TRENDS

- In the UK, a cybercrime or fraud is committed every **4 seconds**.
- The average cost of a breach in the UK in 2016 was **£2.6M** - up from £1.7M in 2015.
- The yearly global impact of cybercrime is \$3 trillion - more than marijuana, cocaine and heroin combined.
This is expected to grow to \$6 Trillion by 2021.

ACCORDING TO KROLL'S GLOBAL FRAUD AND RISK REPORT:

92%

of UK executives experienced an attack, or information loss in the last year, compared **with the global average of 85%**

27%

of companies that use **50 security vendors** or more experienced a breach in the last 6 months. Compared to only **1%** of companies that use **5 security vendors** or less.



Creative ITC

To get further insight into how security services from Creative could help transform your organisation, contact **enquiries@creative-itc.com** or visit **creative-itc.com**