novus
A CAE TECHNOLOGY SERVICES COMPANY

Novus Security-as-a-Service

Proactive monitoring, alerting and security management for your Microsoft environment.

Security-as-a-Service: Cloud Tenant

Security-as-a-Service: Everything

Are you getting the most out of your Microsoft licenses?

Many organisations already have impressive security features built into their Microsoft 365 A5 and E5 software plans, but aren't getting the most value out of existing license investments because their security hasn't been properly configured.

Policies often haven't been set up, alerts might not be in place, monitoring isn't being conducted and new security patching isn't being rolled out.

Novus Security-as-a-Service solution for Microsoft environments helps you to extract **all** the value from your licenses so that you get the most out of your IT investment.

How secure are you?

39% of businesses experienced a cyber security breach or attack last year

83% of cyber security breaches are phishing attacks targeting users

35% of businesses are using security monitoring tools

In the last year alone, 39% of businesses reported a cyber security breach or attack (of which 27% experience an attack every week).

Despite the high number of breaches, only 35% of businesses are using security monitoring tools and just 32% are monitoring user activity. With phishing attacks accounting for 83% of attacks, user monitoring is critical as this is often a business' weakest point. [1]

And with remote working becoming more prevalent following COVID, companies are finding user monitoring and endpoint patching more difficult than ever to manage.

novus
A CAE TECHNOLOGY SERVICES COMPANY

Novus Security: Everything

Novus Security: Cloud Tenant

NSure Backup and Recovery

A holistic approach to security and business recovery

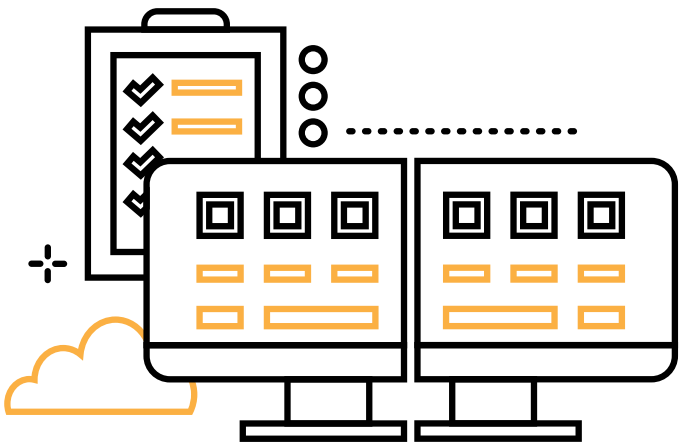
Protecting your organisation isn't just about **buying security solutions or antivirus software.**

It's also about monitoring activity across your IT operations to spot breaches before they have an impact on your business and staff.

It's about applying real-life human thinking to complex security situations to ensure you maintain a balance between staff having the IT freedom to carry out their jobs effectively, and the necessary checks and restrictions being in place to prevent unwanted users gaining access to your valuable data and technology. We deliver this through **Novus Security: Cloud Tenant.**

For increased protection, it's about digging deeper into the security underpinning your on-premise and cloud environments to ensure that you're covered, wherever your applications and data reside - through **Novus Security: Everything**

Ultimately, it's also about having a Plan B if things do go wrong: with all your data backed up safely, combined with the ability to get back up and running as quickly as possible through our disaster recovery service, **NSure.**



novus
A CAE TECHNOLOGY SERVICES COMPANY

Novus Security: Cloud Tenant

Assess
We initially conduct an assessment of your IT estate – both cloud and on-premise, to understand your security landscape and identify any gaps, and compare that with our best practice processes.

Baseline
We put in place a strong foundation of security measures; across policy and software configuration, alerts and monitoring to give you a resilient security baseline.

Monitoring
Once your security foundation is in place, our expert team monitors your environment for any alerts or unusual activity. For straightforward alerts, our team will resolve these issues and alerts on your behalf.

Remediation
Because we have real people sat monitoring your environment, if we get an alert that can't be resolved without your input, we'll contact you to check if the activity we've detected is correct or whether action needs to be taken.

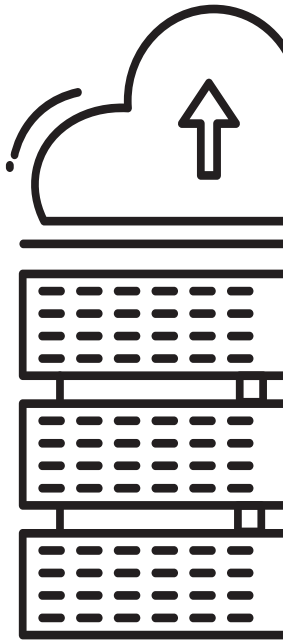
Microsoft Expertise
In addition to monitoring your environment and activity, we wrap around our bespoke experience in managing Microsoft environments for hundreds of customers to overlay our Microsoft policies and best practice configuration rules.

Configuring Microsoft Licenses

Did you know your Microsoft 365 E5 and A5 licenses already come with a number of comprehensive security technologies included?

As part of the Novus Security as a Service: Cloud Tenant solution, we start by configuring your existing Microsoft licenses to achieve a resilient security baseline:

- **Microsoft Defender for Identify** – This leverages your on-premise Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organisation.
- **Microsoft Cloud App Security** - Provides rich visibility, control over data travel, and sophisticated analytics to identity and combat cyber threats across all your Microsoft and third-party cloud services.
- **Microsoft Defender for Endpoint** - An enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- **Microsoft 365 Defender** – Provides the capability for security teams to manage all endpoint, email and collaboration tools, cross-product investigation, configuration, and remediation activities within a single unified dashboard.
- **Microsoft Multi-factor Authentication (MFA)** - Extra security to check users accessing systems from unknown networks.
- **Conditional Access** - Security group policies that incorporate Microsoft Security Baselines and guidance from the NCSC.
- **Office 365 Advanced Threat Protection** - A cloud-based email filtering service that helps protect against phishing, business email compromise, and malware attacks.



novus
A CAE TECHNOLOGY SERVICES COMPANY

Novus Security: Everything

If you're dealing with sensitive data, or if downtime needs to be minimised at all costs, then Security - Everything builds on your Security - Cloud Tenant foundations to add more protection and resilience to your IT, incorporating your on-premise devices into your overall security management package.

Security: Everything includes everything you get in Security: Cloud Tenant plus your on-premise devices.

On-premise IT

Securing your on-premise IT, across end point devices and servers.

- **Microsoft Defender Antivirus** - cloud-delivered real-time protection, using behavioural, heuristics and machine learning to block malicious files.
- **Attack Surface Reduction** - reduces the risky behaviours that legitimate applications can cause.
- **AppLocker** - a whitelisting tool that can be configured to help prevent the infection of malware.
- **Microsoft 365 Defender for Endpoint** - assisting with addressing any endpoint vulnerabilities detected.
- **Security Hardening** – applying Novus security baseline group policies to your IT.
- **External Access Hardening** - restrict IP and domains to block unknown threats and attacks.

Plus...

Included in our Security: Everything package, if an attack does occur, we will parachute in our Rapid Response Team to help you get back up and running.

NSure Backup and Recovery

However secure your IT is, the reality is that the majority of businesses will fall prey to an attack at some point (39% of businesses reported a cyber security breach last year). [1]

NSure is our bespoke Backup and Recovery solution to get you back on track, should the worst happen. Whilst we can endeavour to make your Microsoft environment as secure as possible with our proactive monitoring services, organisations always need a resilient backup and recovery foundation in place.

Using Veeam Backup and Replication technology, we can protect your hybrid IT environment, across on-premise and cloud IT resources to minimise data loss and downtime in the event of a cyber security breach.

Some of the benefits of our NSure Backup and Recovery solution are:

- Eliminate data loss through stringent RTO and RPO
- Reduce impact of ransomware with immutable backups
- Protect any OS and applications that are running within a VMware or Hyper-V environment
- Flexible to match your data needs, but secure and resilient to protect you
- End to end encryption
- Configured, supported and managed by the Novus team

A real life example

We received a call last year from an Education organisation who had been the target of the PYSA ransomware. One of their staff members had unknowingly clicked on a link in an email that contained the PYSA virus, which had then gone on to infect every server and end user device on their network.

Every file on every device across their entire organisation was encrypted, destroying all versioning within Office 365 in the process.

From just one click, over 30 years' of data was lost.

There was no active security monitoring or backup solution in place. Novus had to rebuild the customer's IT from scratch, but they still lost all their data.

If this organisation had used Novus' Security as a Service and NSure Backup and Recovery solution, it would be a very different scenario:

- Novus' security monitoring service would have detected the known PYSA ransomware in the email, preventing the user from clicking on the link.
- If the user had clicked on another link containing unknown malware, Novus would have detected it in the system and contained the virus before it could infect further machines.
- If data did become encrypted, NSure would enable Novus to recover data from a previous backup resulting in minimal data loss.
- If servers or devices became compromised, Novus could immediately start rebuilding systems onsite or at Novus' datacentre.

For more information about how you can improve your own security and resilience, get in touch for an assessment.

novus.co.uk

1 - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021