SOLUTION OVERVIEW

Patching-as-a-Service For Education

Security & Vulnerability

THE PATCHING CHALLENGE

The past twelve months has seen an unprecedented surge in the number of cyber-attacks targeting the education sector. Whereas the National Cyber Security Centre (NCSC) has recommended a 'strength in depth' approach to addressing this risk, the Education & Skills Funding Agency has taken this one step further and made Cyber Essentials Plus a requirement for the 2021 to 2022 funding year.

Patching is a major part of protecting IT environments and achieving Cyber Essentials. Almost two-thirds of all security breaches exploit a vulnerability for which a patch has already been made available; it just has not been applied.

For many education establishments, patching can be challenging, overstretched internal teams, vast numbers of servers and the need to patch out-of-hours all contribute to vital updates being missed. It is not uncommon for teams to fall behind with patch management however, doing so only compounds the pressure on the IT team while exposing the organisations to far greater risk.

HELPING YOU TO CATCH-UP & KEEP PACE

NAK can help you to address the patching challenge. Our experience, know-how and tools enables us to assess your environment and to not only determine what patching is required, but to prioritise this activity to ensure the most critical vulnerabilities are addressed first.

Our methodical approach to patching and ability to conduct this outside of core teaching hours enables us to quickly apply the necessary patches and catch-up to where you need to be without disruption to your organisation or additional burden being placed on your IT team.

Once you are up to date, we can help you to remain so and to keep pace with the flow of patches being provided by operating system and third-party vendors. We continually monitor your environment, keeping a log of each release and patch-level, as well as scanning for security vulnerabilities outside of standard service patch management. We tune into the monthly patch cycles from all of the relevant vendors and prioritise, schedule, deploy and test each of these as part of our managed service.

NAK
JOINING UP THE DOTS

OUR APPROACH

Our extensive experience in this field has allowed us to develop an approach and methodology which is highly effective, and this is supported by market-leading tools that enable us to do this efficiently. Our approach follows four steps:

DISCOVER

We take the time to firstly understand your organisation and the critical nature of your environment and infrastructure. We then utilise our tools to conduct a thorough security and vulnerability assessment of your software, the output of which is a detailed report on your current state of patch compliance.

OPTIMISE

We will then look to streamline your patching process, prioritising against your needs and ensuring that each system is brought up to date and can remain up to date across every server and if required, endpoint.

TRANSFORM

We look to bring discipline and best practice to the management of your patching, having a process that is understood by both parties, is aligned to the way that you work, and that meets the policies and regulations that apply to your establishment.

SUPPORT

We provide you with a fully managed service that can either focus on a particular part of your infrastructure or extend across all of your software. This is backed up by our 24x7 support service that enables us to perform required patching out-of-hours to avoid disruption.

NAK
JOINING UP THE DOTS

OUR PATCHING SERVICE

Whereas we have a standard approach and methodology for our Patching-as-a-Service for Education, we recognise that different establishments require us to support them in different ways. All of our services include Service Delivery Management, we then work with you to tailor a service around our Security Patch Management and Vulnerability Management.

Service Delivery Management

All of our managed services including Patching-as-a-Service comes with Service Account Management.
This includes:

- Designated day-to-day contact for any service-related issues or requests.
- Alignment of our SLA's to your specific needs.
- Monthly reporting on service delivery.
- 24x7 escalation and support via our Service Centre.

Security Patch Management

This encompasses the planning, deployment and management of operating system security and vulnerability updates that are normally released on a monthly cycle. We work with you to fully define the areas of demarcation, but manage the full process that includes:

- Pre and post deployment system monitoring.
- Patch schedule and maintenance windows.
- Deployment testing and sign-off.
- Pre and post deployment validation and reporting.
- Work with you to resolve any server/patch issues.

Vulnerability Management

It is recommended that organisations actively scan and assess for security vulnerabilities outside of standard server patch management. This prevents systems and applications becoming insecure over time and issues around regulatory compliance e.g. PCI DSS and Cyber Essentials.

Our Vulnerability Management Service enables for core infrastructure and applications to be maintained at an agreed version level in order to sustain vendor support and meet any regulatory compliance requirements.
This service includes:

- Review of vulnerability scan output reports.
- Management of remediation, escalation, and deviation of all identified vulnerabilities.
- Regular reporting as part of Service Delivery Management.

KEY BENEFITS

By utilising NAK's Patching-as-a-Service and Vulnerability Management you gain the peace of mind that your environment is being meticulously monitored and patched against a defined service level. This delivers key benefits to your establishment, your end-users and your IT team:

Increase Security

By ensuring you remain up to date with all patching we significantly reduce your exposure to cyber security risks associated with known software vulnerabilities.

Best In Class Automation

You gain the benefit of utilising industry-leading tools to support patch management that is provided as part of our service and removes the need for you to invest in these tools.

Cyber Essentials

By having a meticulous approach to patching that is documented and auditable for Cyber Essentials Plus required for funding.

Improved Visibility

Our service and tools provide you with full visibility into your software estate and you gain the benefit of regular reports showing patch compliance, identified vulnerabilities and remediation action.

Minimise Disruption

By planning and managing a patch schedule and performing tasks outside of teaching hours we help you minimise disruptions to your organisation.

Improved Resource Utilisation

By taking care of this critical housekeeping task, we remove the burden from your internal team, reducing the need to have them work out of hours and free them to focus on other areas where they can add more value to your organisation.

WANT TO KNOW MORE

We would be more than happy to run a short discovery workshop with you to understand your patching challenge and to detail how we can specifically help you. If you want to find out more or have a specific question, please do not hesitate to contact us:

0300 456 0471
enquiries@nak.co.uk
nak.co.uk

NAK
JOINING UP THE DOTS