

BRADFORD CAMPUS MANAGER

Case Study

Customer Higher Education

Durham University
Durham, UK

For its first United Kingdom installation, Campus Manager's anti-virus features substantially reduce infection rate and promotes campus wide Network Authentication for all users and machines.

Environment

A campus network serviced by Cisco switches, HP ProCurve switches, and 100 network servers including HP, Dell, Sun/Solaris, Windows, and Linux currently supporting more than 18,000 students and 4,000 staff nodes.



Challenges

Identify and deploy a campus-wide network access control solution that required both registration – providing a threshold of accountability – and the capacity to check for updated patches of Windows computers before allowing users onto the production network.

Solution

Durham University selected Campus Manager from Bradford Networks, an appliance-based solution that manages, secures, and controls all devices accessing the network while enforcing network authentication and registration policies. This includes identifying, localizing, and tracking network clients quickly, connection-based security scanning, and isolating 'at risk' users and devices in a Quarantine area.



BRADFORDnetworks
Maximizing Network Security

CUSTOMER

- 18,000 students
- 4,000 employees and staff

Durham University is a world-class University with two locations: one in the city of Durham and one in Queen's Campus in Stockton. In both locations the University is engaged in:

- High-quality teaching and learning
- Advanced research and partnership with business
- Regional and community partnerships and initiatives
- Services for conferences, events, and visitor accommodations



The University is collegiate, with colleges providing residential, social, and welfare facilities for their student members, and creating a sense of community for staff and students together. Its academic teaching and research programs are delivered through departments contained within three faculties: Arts and Humanities, Science, and Social Sciences and Health.

ENVIRONMENT

- Cisco, HP, Dell
- Sun, Windows, Linux

Consisting of approximately 22,000 users and 18,000 network nodes (representing 18,000 students and 4,000 employees and staff respectively), the Durham University hardware plant consists of a star-shaped, gigabit backbone based on Cisco routers with mainly HP ProCurve switches at the distribution layer. More than one hundred servers – a mélange of HP, Dell, Sun/Solaris, Windows, and Linux – support the campus' round-the-clock networking activities. The IT staff, which is chartered to provide core infrastructure services to support teaching and research within the University and the provisioning of Information Technology services therein, includes four full-time staff for the network and ten for systems.

CHALLENGES

- Registration process

Network-based viruses that insinuate themselves onto a campus often require extraordinary extrication. The solution applied to them, in turn, can either be reactive and after-the-fact or proactive and anticipatory. And that's true regardless of whether a campus network is located around the corner or, in the case of Durham University, "across the pond." Viruses, it seems, are rarely parochial in nature.

Paul Jones, Head of Systems Information Technology Service at the University, is intimately familiar with the former phenomenon as the march towards the latter evolved. And with approximately 22,000 users and 18,000 network nodes he also knows how prolific and rapidly a virus could spread.

"We had problems with machines that were infected with viruses or weren't patched to an adequate degree in previous years particularly at the start of the school year in October. "

For Jones the problems were exacerbated or exposed as the University moved from a manual registration process based on MAC address to one using "Net Registration," which was more automated.



CHALLENGES

- Network level Authentication

"The majority of PCs on our network were not domain authenticated, especially among the student population, and un-patched and virus-ridden machines caused a host of network problems," confirmed Jones. "It was inevitable at the start of each academic session that we would encounter a large outbreak of 'virus-infected' machines and we would have to run what we called a 'surgery' for students who either couldn't get their machines set up properly or found that once they got them set up they were immediately infected." These events also, according to Jones, placed a modest to substantial drain on the help desk resources themselves.



"We had a large number of calls to the Helpdesk relating to viruses and/or ad/spyware. In many cases, computers were badly infected and needed several hours of work to clean and patch them. On average each call would take 3-4 hours to solve. The Helpdesk staff provided initial help/advice with more complex problems assigned to one of two Customer Services IT consultants to resolve. It really became a labor-intensive exercise."

He continued, "In spite of our best efforts these viral outbreaks occupied many staff for several weeks at a time each year. We needed better network-level security for problem tracing. We needed, ultimately, to provide network-level authentication."

Jones identified a pair of priorities he associated with reliable network authentication, each an integral element to establishing and sustaining a certain defined level of infrastructure integrity to the Residential Network.

"We felt the first element would provide us a way of checking that the machines connecting onto the network were in as reasonable a state as possible; acceptable to the guidelines we had developed. While the anti-virus aspect was important, the biggest issue for us," said Jones, "was to make certain that the machines were adequately patched."

The second was focused more on identifying a solution that would favorably disrupt "business as usual."

"Traditionally we worked on a trusted basis of users contacting us to register the fact they had machines on the network and requesting IP addresses for them from us," said Jones. "For instance, we would have a nominal identification marker, knowing in which department the machine was located, the name of the departmental administrator, and the ability to contact that individual if we encountered some kind of network misdemeanor. It was all based around trust."

However, the more granular information associated with a particular machine or a specific user was not always information that could be used to head off viral outbreaks, remained out of sight, and largely out of reach.

"While it's true we got these machines registered, it didn't give us at all the ability to say, conclusively, that it was a particular user that was actually on this machine, using that address, at that particular time. So, from a network security and network authentication perspective, it was this second thread or priority focused on developing a secure campus that would enable us to establish a viral-free and user-specific network."

SOLUTIONS

- Protecting the integrity of the network
- Enhancing the user experience
- Reducing the cost of supporting the network

According to Jones the search to identify a vendor that would provide immediate relief and mitigation on these central issues was given the code name "Net Vet," indicative of ensuring both user and machine are properly "vetted" before a connection to the network was allowed. The solution selected would also have to be flexible, extensible and support Open Standards while also permitting interoperability within a multi-vendor configuration. The formal tendering process to potential suppliers was based on preliminary discussions around these requirements, as well as the ability to respond to all of the network's issues at that time including:

- Lack of anti-virus software or regular updates
- Lack of anti-spyware or regular updates
- Lack of recommended service packs (i.e. Microsoft critical updates)
- Lack of personal firewall
- Devices spoofing DHCP or having Bridging enabled

In turn, the selected vendor would enable:

- All users to be authenticated to the Network.
- All devices checked for anti-virus, anti-spyware protection during the network login process.
- Devices that failed to meet the minimum requirements of the Acceptable Use Policy would be automatically switched to a Quarantine network and provided with information as to why the device failed and opportunities to remediate the problem online or to contact the University Help Desk.

Ultimately, the solution would protect the integrity of the network, enhance the user experience, and significantly reduce the cost of supporting the network.

Working with Khipu Networks, a Hampshire-based advanced systems integrator focused on supplying innovative, secure, and compliant infrastructure solutions across the public and private sector, Jones assembled the proposal document. Only a few weeks later, following evaluations of several NAC associated vendors, Jones and his team selected the Bradford Networks' Campus Manager solution. "The outcome," Jones said, "was inescapable."

"In practice there wasn't anything else which fit our requirements as closely," said Jones. "It was flexible enough to fit our routed view of network provisioning and didn't force its own architecture upon us. Other commercial offerings in this area were just not as capable or forgiving."

When it came down to selecting Campus Manager, Jones' particular view of routing also made his decision and that of his team's much easier.

"One enormously important thing from our point of view was Campus Manager's flexibility as a solution. The way we have our network set up presently is in a traditional, star-shaped topology with routing occurring between the center and the edge routers. We wanted to route from the edge back into the center, without resorting to extending VLANs back into the core, and we were able to continue to operate that way. In a sense we knew we had to make some changes to the network but the amount of changes that we were required to make when we installed Campus Manager was actually quite small." Working closely with the Khipu team, who have extensive experience within Campus and Halls of Residence networks, everything went according to plan.

SOLUTIONS

- Out-of-band Architecture
- VLAN Switching

Campus Manager's VLAN specific architecture amplified, for Jones, the virtual transparency of the solution itself.

"We obviously had to put the VLANs in at the edge of the network in order to provide the separation from the edge switches out to the desktop. Other than that we didn't have to make any further changes to the layout or architecture at the core of the network."

Additionally, Jones and his team were impressed with Campus Manager's out-of-band architecture.

"Aside of when the initial vetting of the client was being undertaken we wanted the solution to be as lightweight as possible," said Jones. "This covers two major factors, clientless operation and out-of-band management. Other suppliers solutions, which were based around semi-permanent in-line solutions, were not considered appropriate. A centralized solution was deemed far more satisfactory to us than a distributed one, which might involve supporting a large number of control elements around the periphery of the network."

Having placed his faith and capital investment into Campus Manager, Jones quickly adopted the solution's Usage Policy Management features (enforcing network acceptable use policy) and Access Control Management (controlling unauthorized access to the network by promoting and enforcing registration policies for all devices on the network and authorization policies for all users on the network).

Jones continued, "This is the primary reason for adopting Campus Manager. The flexibility of Campus Manager enabled us to configure it around our existing network architecture rather than imposing its own structure. For example we did not bring VLAN segmentation right back into the core of the network. We continued with VLAN separation at the edges but with a routed structure into the core, using access control lists on backbone routers to limit client visibility to external resources. Fortunately Bradford was able to accommodate this relatively easily and we did not need to do a significant overhaul of our network in order to implement it."

BENEFITS

- All users authenticated
- All devices validated

For Jones the experience of implementing and deploying Campus Manager has been conclusive and compelling.

"For one thing there is an enormous reduction in the number of infected machines and fewer helpdesk calls about the number of viruses and infected files. Also, now that we've rolled out Campus Manager to the student network (approximately 6,000 machines), trust me when I say that it's been a much happier experience at the start of this academic year than previous ones."

Jones also has seen Campus Manager make a significant impact in the area of unpatched machines and, longer term, he sees making more use of its network level authentication features across the whole of the network.

"The IT Service can now be confident that the machines managed by Campus Manager will have recognized anti-virus and ad/spyware applications installed. Additionally, any Windows computers will be up-to-date with the latest security patches and service packs," said Jones.

BENEFITS

- Installation with no disruption to network services

He added, "Finally, and most significantly, the IT Service can now easily block access to users' computers when the need arises. Such as a computer that is infected can be blocked by IT staff, forcing the user to take required action in order to regain access to the network."

Happily, Jones has also begun the task of bringing Campus Manager "to the masses" not yet converted to the epistle of network authentication.

"We've begun rolling out Campus Manager functionality to fixed desktop machines in academic departments, as opposed to the student network, which was of course, our initial focus," said Jones. "Our goal to provide secure, campus-level network authentication for all users and machines accessing our network is, thanks in large part to Campus Manager, fully and finally within our grasp and achievable."

"The installation of our first Campus Manager deployment was a great success," stated Matt Ashman, Commercial Manager – Khipu Networks, working in partnership with the Durham team. "We successfully deployed the solution into a pilot area then across the entire student network, with no disruption to network services. The success of the Durham University project has enabled us to work with over 20 institutions throughout the UK and Ireland, implementing Campus Manager into Campus and Halls of Residence wireless and wired networks."

Benefits Gained From BRADFORD CAMPUS MANAGER

- All users authenticated to the network.
- All devices checked for anti-virus, anti-spyware protection during the network login process.
- Devices that fail to meet the minimum requirements of the Acceptable Use Policy automatically switched to a Quarantine network and provided with information as to why the device failed and opportunities to remediate the problem online or to contact the University Help Desk.
- Its flexibility and lightweight footprint has enabled the University to configure Campus Manager around its existing network architecture rather than incorporating and enforcing its own proprietary operational strictures.
- The ability, over time, to rollout network authentication for all users and machines, students and staff alike, across the entire campus network.