

BRADFORD CAMPUS MANAGER

Case Study

Customer Higher Education

University of Kent
Canterbury, UK

University of Kent deploys Bradford Campus Manager to actively control and manage their student residence network and network vulnerabilities through secure registration and identity management, reducing operational intervention and promoting student satisfaction.

Environment

The University of Kent network is a star topology with gigabit ethernet interconnects to edge switches and 10/100 ethernet to users. With HP servers cascading to 166 24 or 48 port HP switches serviced by Cisco Routers at the core, the network supports approximately 15,000 students and up to 2,000 staff.



Challenges

Extend, improve, and automate the University's Study Bedroom Network Service to ensure supply meets demand, enabling students to connect as soon as they arrive on campus. Reduce or eliminate administrative overhead, including help desk intervention, while refining the device registration process for students and internal stakeholders alike.

Solution

University of Kent selected Bradford Campus Manager, a user-centric, network-based NAC solution with integrated identity management, endpoint compliance and usage policy enforcement capabilities. The solution actively monitors and controls network users and devices to provide enhanced security within the network. Through the enforcement of network usage policies, the solution ensures the network is safe and secure.



BRADFORDnetworks
Maximizing Network Security

CUSTOMER

- 15,992 students
- 600 academic & research staff

The University of Kent is a UK higher education institution founded in 1965 and funded by the Higher Education Funding Council for England. The Higher Education Funding Council for England (HEFCE) distributes public money for teaching and research to universities and colleges. The University has three associate colleges: Canterbury College, Mid-Kent College and South Kent College. The main campus is the University of Kent at Canterbury covering 300 acres just over a mile from Canterbury's city centre. The University is divided into three faculties including Humanities, Social Sciences and Science, Technology and Medical Studies (STMS).



As of December 1 2006, 15,992 undergraduates and post-graduate students attended Kent and its campuses in Medway, Tonbridge and Brussels, along with some 600 academic and research staff.

ENVIRONMENT

- HP
- Cisco

The University of Kent network is a star topology with gigabit ethernet interconnects to edge switches and 10/100 ethernet to users. With HP servers cascading to 166 24 or 48 port HP switches serviced by Cisco Routers at the core, the network supports approximately 15,000 students and up to 2,000 staff in parallel. The student residence network has nearly 4000 wired connections in their rooms.

CHALLENGES

- Kent's Study Bedroom Service (SBS)

At University of Kent both the global – as well as the nearby village – are available from the comfort and convenience of student residence halls. Accessing either, however, is another matter entirely.

Kent's Study Bedroom Service (SBS) provides a network service which connects the majority of study bedrooms on campus to the main University network. From a student's room, they can access e-mail, networked file stores, course material, library resources as well as Internet services using their own PC. This includes:

- Web sites
- E-mail and communication
- Newsgroups
- Networked printers
- Kent file stores
- IPTV

Viruses
Adware
Spyware



"In order to access the SBS Service, each student is supplied with a 'how to' booklet that serves as a guide to securing and registering their computer," said Jim Higham, the University's Help Desk Manager. "This handbook includes regulations, information on malicious software and a Health Check CD, containing a range of advice and software designed to help students keep their computers secure and safe from malicious software such as viruses, adware, and spyware."

CHALLENGES

- Registration Process

To accentuate its significance, in the preamble to the actual registration process, the handbook describes the current state of viruses and their impact on the University at large:

In recent years, there has been a large increase in the amount of malicious software on the Internet. Such software can pose a risk for the University's network and resources and for students and staff who connect their own computers to the campus network. If you do not have an anti-virus checker installed to protect your PC against harmful software, you may experience problems if your computer becomes infected. We recommend you follow the instructions here carefully. If your PC is found to be vulnerable to viruses or security issues, your access to the network may be restricted or withdrawn.

In the simple process that follows, students can register their PC's for access to campus network services and internet access by opening a web browser and following the on-screen instructions:

Study Bedroom Service Website | Securing your PC
Study Bedroom Service

Registration Process Part II - Microsoft Windows

Before proceeding, please ensure you have secured your computer by either using your Computing Health Check CD, or by visiting the [Securing Your PC](#) webpages.

To activate your study bedroom connection please enter your details in the boxes below and then follow the instructions beneath.

Please note that all registration attempts are logged.

Username: <input type="text"/>	These are your Kent Computing Account username and password. Students - claim your computing account now if you haven't already. Conference guests may ask their conference organiser or Computing Service Reception for an account.
Password: <input type="password"/>	
Student Number: <input type="text"/>	This is your 8-digit student number as shown on your student card. Conference visitors, please enter the word conference and staff please enter the word staff .
Corridor/House and Room Number: <input type="text"/>	For example: 4 Room A, N4E Room 3, or C1 Room 5
College / Court: <input type="text" value="Select from list:"/>	

Assuming you entered the correct details above, you will be prompted to download the CSA tool. This will be used to ensure your computer is secure to join our network. Please follow these instructions:

1. Fill in the details requested above
2. Click 'Proceed' and download the tool to your Desktop
3. Minimise your web browser and locate the icon for the CSA tool
4. Double-click on the tool to begin the scan

Students enter their user name and password so the university knows who they are. Following an easy to do scan of their computer to check for vulnerabilities and the presence of operating system and AV updates and AV software, a screen similar to the following appears if the registration is successful.

CHALLENGES

- The enforcement of security prior to connection



If the student experiences problems or if the registration has not been successful, a relevant screen appears offering advice on how to resolve the issue, depending on what the issue is. If all else fails, their handbook has FAQs and contact details for support, but the vast majority connect easily and are up and running within minutes, contacting friends and family back home.

Behind the scenes Kent employs Bradford Campus Manager that allows students to connect quickly and safely as soon as they arrive, with help available online to guide them if their machine needs to be made secure before it connects.

"The enforcement of security prior to connection reduces the risk to each student from other machines, as well as ensuring that their own machine is at minimum risk," said Higham.

He added, "The data collected by BCM is available to support staff, and can help diagnose problems when students visit for help. We are able to track the type of OS used and numbers of machines using the network easily, and can use this to inform our planning and support."

According to Higham, Bradford is also integrated into the long-term goals for the SBS service.

"Our migration to BCM helped us achieve our planned aims of extending and improving the SBS service to ensure supply meets demand such that students can connect as soon as they arrive, and to provide facilities which are easy to use – no prior application is now needed. Further work this year to refine the registration process will improve ease of use further. This includes online access to fuller instructions on our main web site, and online access to University licensed anti-virus software, previously distributed on CD, but now available via password controlled access on the network, prior to full connection," said Higham.

For Higham, whose Information Services Group provides IT, Library, and Business Systems infrastructure and services for the University, having a full-time, automated Network Access Control solution in place has enabled the University to put much of its historical adhoc approaches to network security to rest.

CHALLENGES

- Acceptable Usage Policy

As for the campus Acceptable Usage Policy (AUP), the enforcement of policies was entirely dependent on disabling the student's IT account, clearly not the most prudent or forward-looking solution given the student's eventual need to access IT services in satisfying curriculum.

"Our legacy system was very labor intensive, requiring manual input of data for each user. New year rollover meant that students were unable to connect for the first few days after arrival. Virus and spyware problems although reducing, were still causing start of term support and network issues," said Higham. "We wasted time dealing with virus infections, disabling and re-enabling accounts, and calling people in to have their machines checked before putting them back on."

Higham and his staff believed there had to be a more effective solution, one that protected services and students alike.

Ideally, we wanted students to be able to connect as soon as they arrived, and to reduce or eliminate the admin overhead, but did not have the manpower to develop a new solution.

"Ultimately, we wanted an automated solution where everything is handled online and the user knows what is going on and what they need to do, without visiting us, unless they need help from us of course," said Higham.

SOLUTIONS

- Automated Registration Process

Having determined that automation of the registration process with the ability to evaluate the security of connected equipment was paramount to their needs, Higham and members of his Information Services team initiated their search.



"We examined the market for solutions and tested these against our needs and, in particular, our desire to minimize development time for our staff," said Higham.

While the search yielded several vendors of interest, ultimately Higham – working with Khipu Networks, a Hampshire-based advanced systems integrator focused on supplying innovative and secure solutions within the Education market, – concluded that the only real solution favored Bradford Networks in general and Campus Manager in particular.

"They were the only full fit solution," said Higham. "They had a solid track record in US Universities and in their short time in the UK in higher education had demonstrated themselves to be worthy of every consideration as a network access control solution for campuses like ours."

For Higham, the dividends in deploying BCM were consistent and reliable.

"For example, better service for students and more customer friendly handling of AUP enforcement as a result of insecure machines," said Higham. "From the operations side of the aisle BCM lowered support costs and there was less of a need for operations to intervene."

SOLUTIONS

- Identity Management
- Endpoint Compliance
- Usage Policy Enforcement

Identity Management

Ensuring network integrity begins by enforcing robust policies and rules. Campus Manager requires all users to register prior to allowing them access to the network, which allows administrators to:

- Control network access for wired, VPN and wireless users
- Assist in tracking all users by location, name or address (MAC and/or IP)
- Provide role-based access and levels of service via dynamic VLAN assignment

All devices that connect to the network are placed in a Registration VLAN until the device is properly registered. Another layer of protection requires the user to authenticate before connecting to the network. Each user and device on the network is registered and tracked to enhance security and access control. Role-based access functionality ensures that users are connected to specific VLANs depending on the type of service authorized. The result is tight control over the network and a consistent, real-time view of activity.

“Our old in-house system aimed to require registration of all equipment connected to the network. However, moving unknown hardware to a separate VLAN which has no network access is more secure than simply not giving an IP address – we have a record of the kit. It also explains to the customer on-screen what has happened and where to get help,” said Higham.

Endpoint Compliance

Campus Manager uses dissolvable and persistent agents to ensure that the computing devices on the network meet minimum required security standards and that the network is safe and secure. The agent will perform registry-based scans on each network device prior to being placed on the live network.

Devices that are ‘at risk’ are placed in a secure Quarantine VLAN where they can remediate the issues without helpdesk intervention (self-help).

- Check anti-virus application type and definition version levels
- Check to ensure anti-spyware applications are installed
- Connection-based scanning upon network access

“We have had serious virus problems in previous years,” said Higham. “These caused problems with using the network, as well as increased demand for helpdesk support. Ensuring that AV software is installed and up-to-date has reduced this significantly.

Campus Manager’s endpoint compliance functionality performs three significant functions:

- Every device is checked before being allowed to connect to the production network
- Non-compliant ‘at risk’ devices are isolated in a “Quarantine” area
- The Remediation Center provides ‘self-help’ services to resolve issues without helpdesk intervention

SOLUTIONS

- Identity Management
- Endpoint Compliance
- Usage Policy Enforcement

Usage Policy Enforcement

Campus Manager is a powerful tool to help enforce the network's acceptable use policies. Whether it is tracking unwanted activities, such as gaming, music file sharing, or instant messaging, the functionality in Campus Manager will help to enforce specific network policies to ensure that clients on the network do not abuse services. Using scheduled scanning, the solution applies role-based identity information to ensure policies are user-specific. This approach integrates all identity management and endpoint compliance with usage policy to ensure optimum performance.

Campus Manager interfaces with third party solutions like traffic shapers and IDS/IPS solutions to gather critical information to determine if network violations are occurring. The result is identification, notification, problem isolation and corrective action. The solution allows network administrators to:

- Enforce acceptable network use policies
- Control chatting, gaming and file sharing
- Limit bandwidth usage
- Interface with IDS, traffic shapers, and other external devices

The Benefits

- Connect easily quickly and safely

For Higham the long and short of Bradford Campus Manager's value to the University reduces to three simple elements:

1. Students are now able to connect as soon as they arrive.
2. Lower administrative and support costs
3. Fewer virus problems

For Higham the resulting savings in administrative time, particularly lower support costs, have made a significant difference in managing the campus network.

"Network access control is now managed automatically without significant administrative or operational input, and our customers are able to connect easily and quickly" said Higham. "On that basis alone Campus Manager has proven its worth."

Higham plans to expand the BCM system to match the growing number of networked student rooms, and is considering the needs of students who require more remote, transient access on campus.

"Control of our wireless networks may be considered in the future to reduce problems associated with vulnerable machines," said Higham. "After all, it's not just hardwired machines that have a monopoly on viruses and taking steps now, before problems occur, ensures our campus and students alike remain safe and the integrity of our network is maintained."

The Benefits

Benefits Gained From BRADFORD CAMPUS MANAGER

- Network access control is now managed automatically without significant administrative or operational input.
- Manually disabling and re-enabling student accounts at the Information Services level eliminated and replaced with an automated, turnkey solution managed by students.
- The enforcement of security prior to connection reduces the risk to each student from other machines, as well as ensuring that their own machine is at minimum risk.
- Data collected by BCM is available to support staff, and can help diagnose problems when students visit for help. BCM easily tracks the type of OS used and number of machines using the network, and Information Services can use this data in its own planning and support.
- Insecure operating systems are prevented from connecting to the network.
- Identity management controls enable Information Services to know who was where on the network – and when.
- Unknown hardware quarantined to a separate VLAN with no network access, preserving network integrity and security.
- Actively controlling and managing vulnerabilities results in fewer support needs and greater customer satisfaction.

About Khipu Networks Limited

Khipu Networks are a UK based advanced systems integrator, focusing on supplying innovative secure compliant infrastructure solutions across the public and private sector. The company is a leading adopter of new and best in breed technology, expert technical staff ensure that customers get the solutions they need, when they want them and how they need them. The ethos is to ensure that the customer has the edge on the security and compliance of their network and not the attacker. Hampshire based Khipu Networks Ltd are the security division of the White Clarke Group of companies.

www.khipu-networks.com

