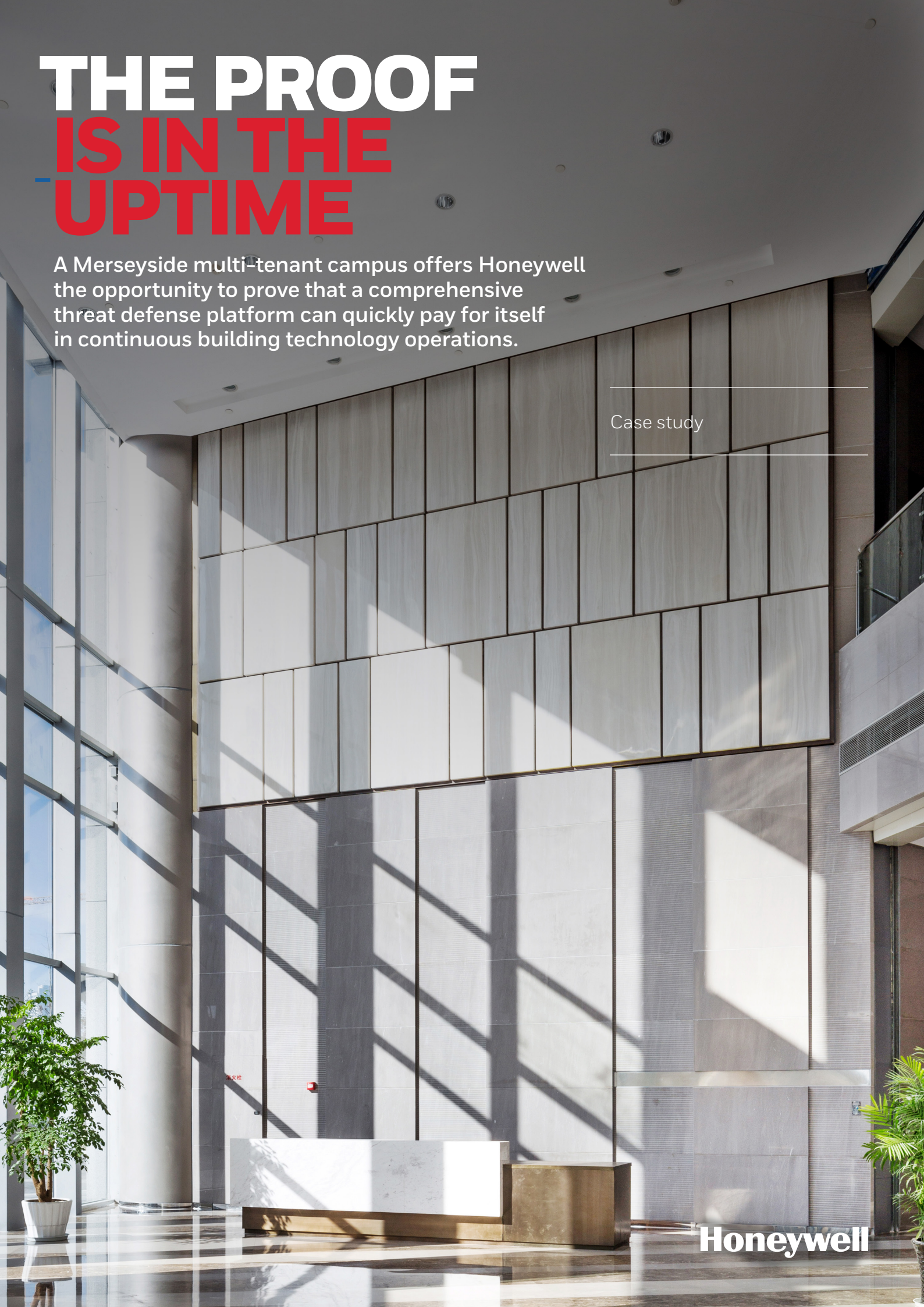
THE PROOF IS IN THE UPTIME

A Merseyside multi-tenant campus offers Honeywell the opportunity to prove that a comprehensive threat defense platform can quickly pay for itself in continuous building technology operations.

Case study

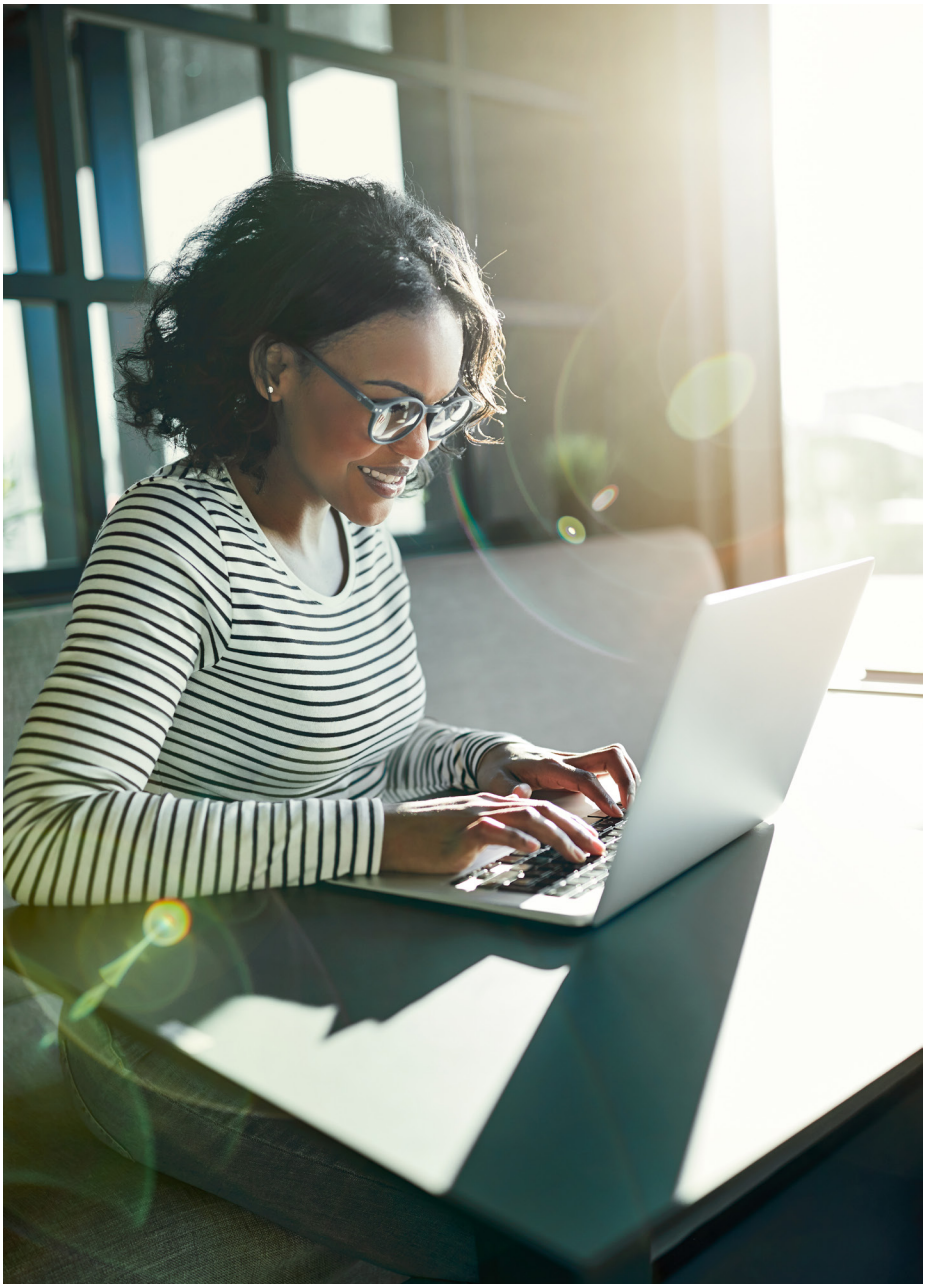


Honeywell

MINIMIZING THE VULNERABILITIES IN OPERATIONAL SECURITY

The customer site featured Enterprise Building Integrator as well as fire, digital video management, access control and intrusion systems from Honeywell.

And as a recognized leader in both building management systems and cybersecurity, this offered Honeywell the opportunity to pilot its pioneering threat defense platform for operational technology systems as well. A successful proof of concept would mean an ongoing contract, and the possibility to expand the service into more properties in the customer's portfolio. There were also financial penalties for underperformance, so the stakes were high, but the Honeywell team of experts was confident.



THE NEEDS

- Reduce the business risk and negative financial impacts of a cybersecurity breach
- Identify threats before they become a costly breach
- Respond to known and unknown threats
- Simple to deploy
- Scalable so that following a successful proof-of-concept it can be expanded across properties
- Meet uptime performance metrics to avoid penalties

THE SOLUTION

One of the site OT Systems was selected for the test. Honeywell deployed the Threat Defense Platform (HTDP) using a cloud-based deception center with virtualized HTDP sensors to cover all the nodes of the tenant's building management system. HTDP was easily deployed within three hours following a simple review of the targeted operational technology network.

The test involved projecting a variety of OT and IT decoys using a single virtual sensor into multiple subnets/ VLAN without any major changes to the network. Breadcrumbs and baits were deployed on the real systems. Then email integration was configured to send alerts.

THE STAKES

The performance incentives for a successful test were based on strict uptime expectations for operational systems. For example a recording disruption of all 85 cameras across the site for just 1 hour would have cost around $88 thousand in penalties to the property owner. Taking into account the cost of the installed system, this meant avoidance of just one such event would result in a return on investment of about 250%.

THE RESULTS

Installation was as simple as expected, with a VM appliance deployed along with network changes locally. Honeywell managed cloud elements and decoys, and the two worked seamlessly. The system passed all its tests with no unmitigated breaches, and expansion into additional spaces and sites will involve only minor network changes and additional decoys.

Most critically, the benefit to the customer doesn't stop at monitoring and alerts, but includes automated active response to cyber attacks, stopping cybersecurity breaches in many cases before anyone is aware of the attempt.

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
buildings.honeywell.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell