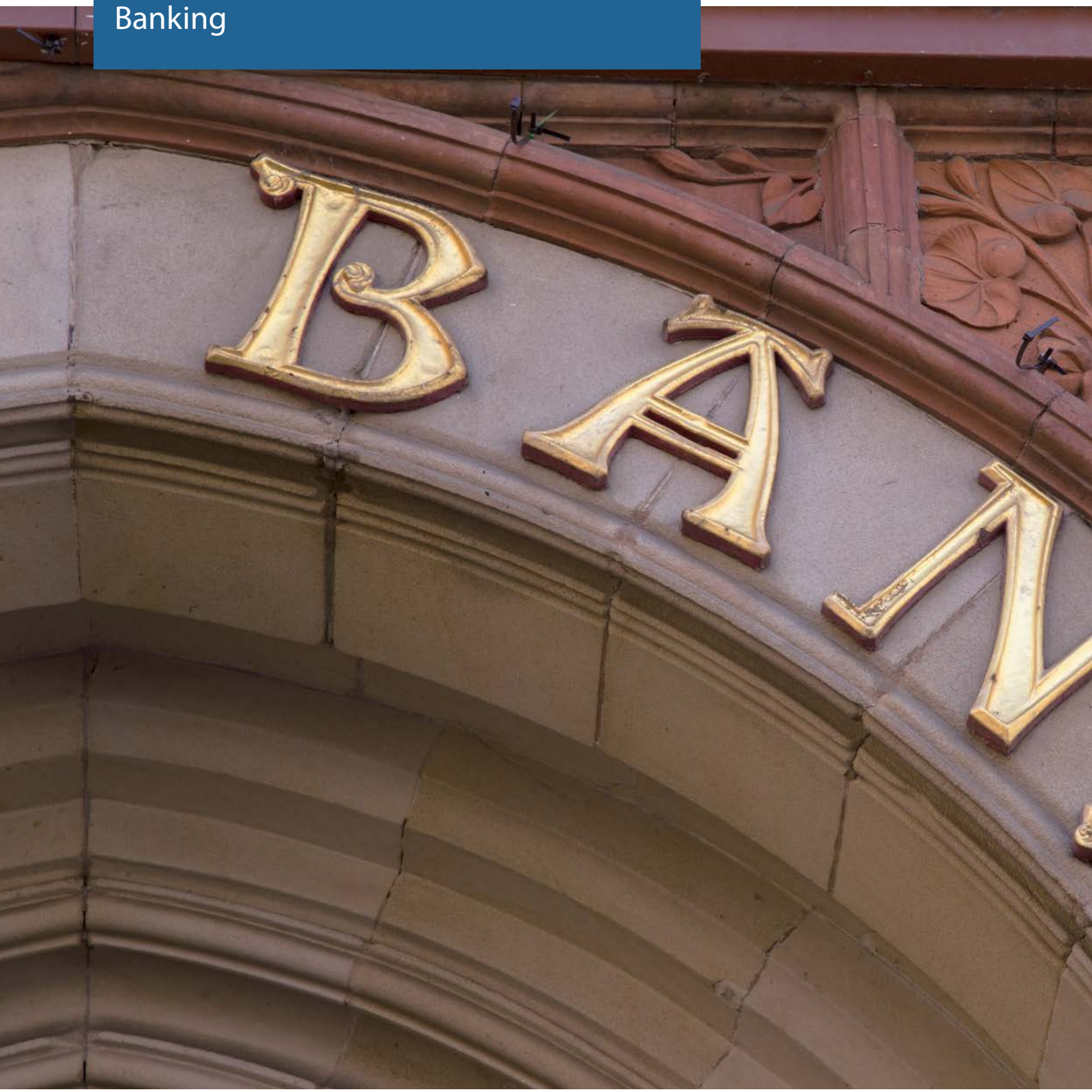
vehere

Case study

Banking



vehere

PacketWorker's innovation has turned it into an essential device for security teams attempting to comprehend the scale of their network, observe activity levels and detect potential shortcomings. Machine Learning plays a key role in defending assets from cyber-criminals and malicious insiders.

Summary

Industry/Organisation

Banking

Challenges

- Comply with regulatory and audit requirements
- Attain comprehensive visibility
- Secure organisation from breaches, data thefts and malware/zero-day attacks
- Reduce complexity with security analytics adoption

Solution

PacketWorker 10G (combined with professional services)

Benefits

- >50% improvement in detection efficiency
- >60% time optimisation for investigations
- >30% reduction in risks associated with data breaches
- >90% reduction in compliance efforts

vehere

"Insider threat is one of the most serious threats a company can face. We knew we needed to prioritise, reduce, and manage cyber security risks to address the needs of our business."

- Name withheld, R1

Background

The contemporary world is witnessing customer expectations, technological capabilities and regulatory requirements join forces with demographic and economic factors to bring about radical changes. This has caused banking institutions to look for ways and means to get used to these changes and adopt a proactive approach towards security. Financial institutions will always be prime targets for cyber-criminals, making their security requirements extremely complex.

This case study focuses on a large global bank and will be referred to as R1 for the sake of anonymity. The bank's intelligence data was facing significant cyber threats from multiple sources. However, despite implementing multiple security protocols, R1 continued to suffer security lapses. The bank's business operations were getting impacted each time such an incident was happening.

Business challenges

Due to a growth in its customer base and burgeoning data usage, R1's ability to respond to these increased risks from malicious insiders and unknown vectors/ exposures, had been severely hampered. R1 needed to manage this ever-growing, ever-changing array of risks from across the globe while ensuring adherence to stringent regulatory requirements. The challenges included:

- Preserving customer trust by protecting data privacy.
- Maintaining strong security without impeding business operations.
- Ensuring compliance with regulatory requirements.
- Adding new devices and introducing services to networks devoid of security monitoring or any understanding of exposure.
- Accommodating bring-your-own-devices and guest end-points without compromising on security.
- Combining existing security tools into cohesive solutions that accelerate incident-response times and reduce vulnerabilities.

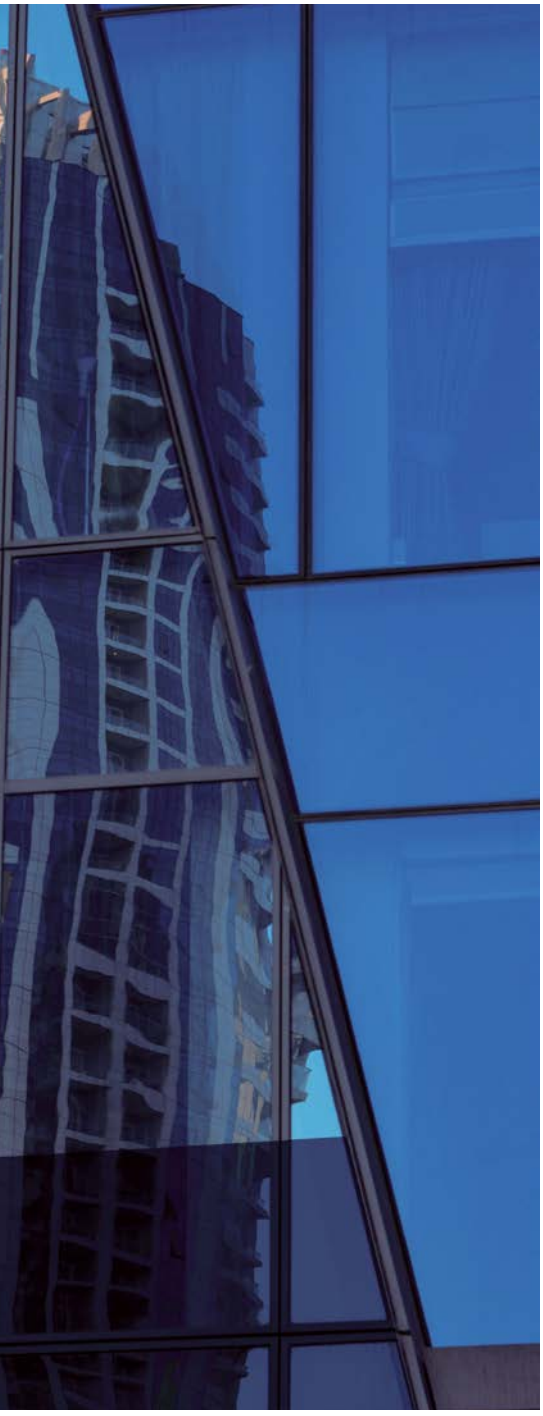
Regulations regarding technology and information security are far-reaching and include areas such as e-mail, SWIFT-coded payments, cipher suite strength, domain name systems, core banking solutions and, back-office applications. R1 recognised a need to proactively defend its sensitive information across the technological value chain. Therefore, R1 undertook a decisive initiative to implement technologies that could help it make sense of the 'unknowns' and provide tangible answers during investigations.

If there was a targeted attack and R1's computers were to become affected, it would have resulted in business disruption and potentially lead to privileged information getting leaked. R1 needed to urgently respond to incidents that required sourcing specialists from external agencies to assist it with time-consuming and risky processes. Thus, the impact of any incident could have amplified. R1 needed an integrated solution that would allow it to maintain staff productivity, ensure threat detection and facilitate rapid response and recovery.

vehere

"PacketWorker's technology gave us visibility into potential implementation differences and policy discrepancies. Leveraging its technology, we were able to identify and remedy these differences before connecting the two networks, mitigating potential integration risks."

- Name withheld, R1



Solution – PacketWorker 10G

Traditional tools that are programmed to spot known threats are no longer sufficient. Modern network border defenses, such as firewalls, perform an important function. However, insiders often escape restrictions imposed by these perimeter security controls.

Limitations posed by legacy approaches

- Perimeter controls are dependent on signatures, rules and heuristics and, hence, are likely to miss attacks at points-of-entry.
- End-point security controls rely on signatures and fall short when it comes to detecting rogue behaviours or detecting unknown attacks.
- Sandboxes are side-stepped by modern attacks, which recognise when they are in a fake space and delay the execution of malicious activities.
- Log tools and security information and event management databases require inordinate amounts of manual effort to ensure data is consistently collected across the entire organisation and matched against the security team's predictions of threats. Besides, not every actor needs to target assets holding the 'crown jewels', they wish to simply exploit the chain of trust.

To combat these challenges, R1 deployed PacketWorker 10G at the core and peripheries of its network. After a prompt installation and using the deep packet inspection and analytics capabilities of PacketWorker 10G, R1 gained complete visibility of its entire infrastructure, including IoT and non-sanctioned devices. Using PacketWorker 10G, the security team was able to identify anomalous activities and disrupt them early, before any damage was done.

PacketWorker 10G's innovation has turned it into an essential device for security teams attempting to comprehend the scale of their network, observe activity levels and detect potential shortcomings. Machine Learning plays a key role in defending assets from modern cyber-criminals and malicious insiders. The technology detects threats and abnormalities emerging across the network on a real-time basis, including insider threats and 'unknown unknowns', enabling the security team to disrupt attacks before they can cause much harm.

Whenever any anomalous behavioural changes happen within the environment, PacketWorker identifies them and alerts the organisation. Changes that are not real threats are fused into PacketWorker's evolving understanding of normality. The arithmetic inside PacketWorker makes it uniquely equipped for featuring noteworthy potential threats without burying them beneath numerous unimportant or repetitive alerts. Going beyond setting down simple rules applicable for network traffic, it can correlate numerous inconspicuous trends isolated by type or time to sniff out real emerging threats and ensure that security analysts are not burdened with false positives.

Benefits - visibility and answers

Equipped with Vehere PacketWorker, R1 can autonomously defend itself against pernicious cyber-criminals and insider threats. Since it does not rely upon any prior assumptions of what 'bad' entails, the self-learning solution is also uniquely capable of identifying hitherto unseen threats.

PacketWorker empowered R1 to deal with cyber threats on a real-time basis. It allowed the security and risk management teams to proactively assess cybersecurity postures and lay down rules to detect malicious behaviour besides using advanced predictive analytics to spot 'unknown unknowns' without disrupting ongoing business processes.

vehere

"R1 has been able to maintain stringent compliance with industry regulations since PacketWorker was implemented. The platform provides real-time anomaly detection capabilities and unprecedented visibility that is simply unmatched by any other vendor in the industry."

- Name withheld, R1

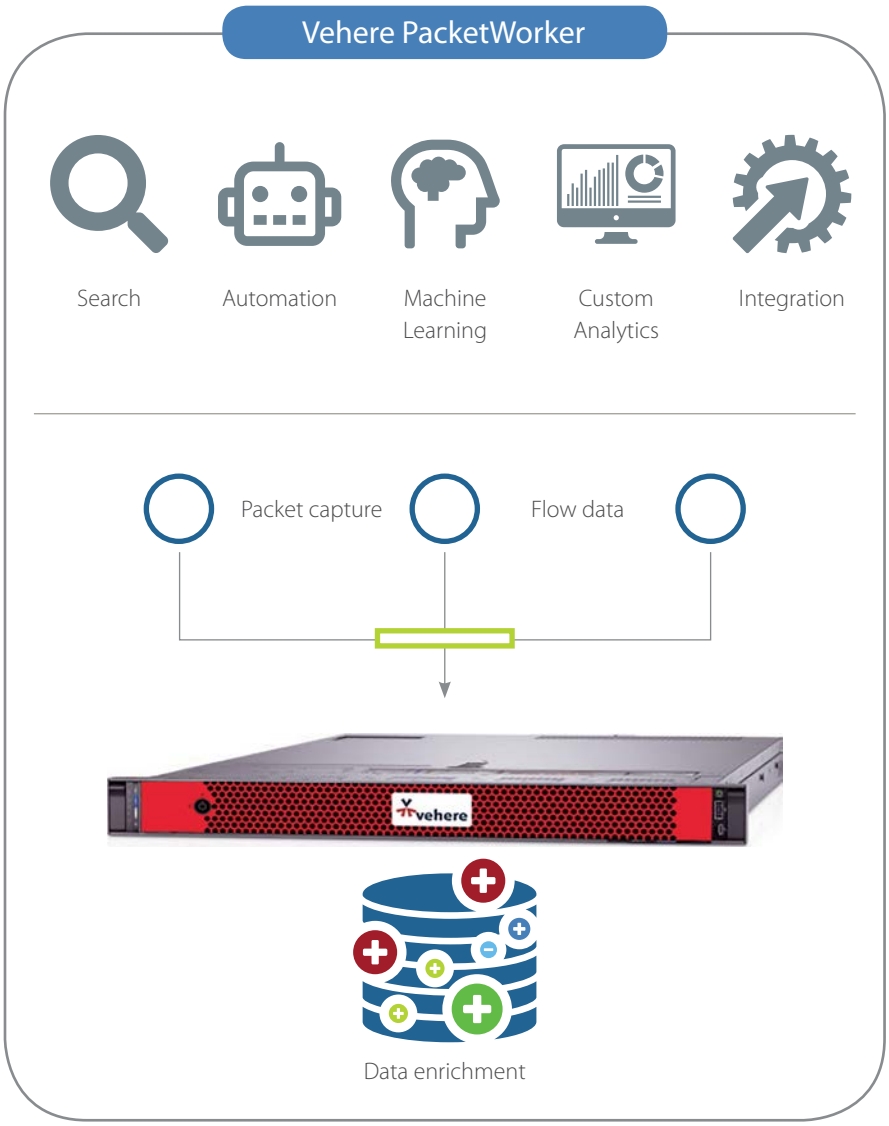
Results

- Faster detection of internal breaches and compromised customer.
- Reduction in incident response times.
- Fewer resources required to manage and act on risk assessment.
- Seamless detection of unknown and insider threats.

With PacketWorker 10G, R1 managed to speed up triage from an average of five days to less than six hours. By simplifying an analyst's interaction with network data and using an easy point-and-click interface to lay down complex behaviour-based rules, enabled the security operations team was imbued with the ability to deliver predictable and repeatable outcomes (irrespective of the skill set of the user), maximising efficiency and significantly reducing dwell-times.

Over time, R1 was able to identify and alleviate threats with greater productivity compared to the same period during the previous year.

PacketWorker facilitated simplification of implementation of big data-led security analytics in security operations by leveraging readily-available structured data from the source of truth – packets on the network.



"We no longer live in an era where cyber-attacks are limited to the desktops or servers. PacketWorker's Machine Learning fights the battle before it has begun."

- Name withheld, R1