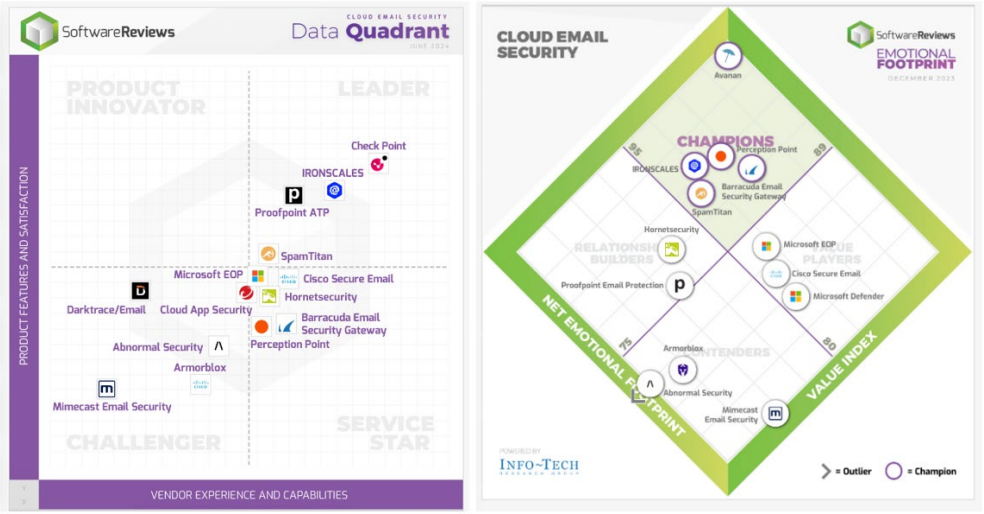
INFO~TECH
RESEARCH GROUP

Hornetsecurity: Redefining Email Security With AI and Global Insights

Carlos E. Rivera

Principal Research Advisor,
Info-Tech Research Group

Hornetsecurity has distinguished itself in our integrated cloud email security (ICES) quadrant with its advanced email security platform. Its solutions are built on next-generation ICES functionalities, showcasing innovative technologies and approaches that tackle the evolving landscape of email threats. My discussions with numerous email security vendors highlight Hornetsecurity's standout features like its robust phishing detection, adaptive data utilization for AI enhancement, and the flexibility of its deployment models. In addition, my Hornetsecurity contact, Adrien Gendre – CPO of the group – was extremely knowledgeable on collaboration tool security, as evidenced by his deep understanding of collaboration security risks, and how its platform operates at the core in comparison to competitors. I learned a considerable amount from Adrien.



Source: ICES Quadrant, Software Reviews, 2024

Company Background and Market Positioning

Hornetsecurity has established itself as a pivotal player in the email security sector, focusing on advanced threat detection and management. Its product offerings are tailored for a diverse clientele ranging from individual business customers to large enterprises, including partnerships with prominent distributors, VARs, and managed service providers. This wide market reach is underpinned by a robust technological

foundation that includes the integration of sophisticated tools like AI, machine learning, and computer vision to detect and counteract threats such as account takeover (ATO), vendor email compromise (VEC), and business email compromise (BEC). Hornetsecurity's approach is holistic, employing a blend of social graph analysis, heuristic algorithms, and sandboxing to ensure comprehensive email security.

The company's strategic positioning involves two main avenues: direct sales through a network of distributors and service providers like TD SYNNEX and Pax8, and integration into the portfolios of broader solution providers such as ISPs, mail services, and tech giants like Cisco and NTT, indicating a strong global presence and adaptability. This dual strategy broadens Hornetsecurity's market reach and enhances its threat intelligence capabilities by leveraging data from over 1.4 billion mailboxes worldwide. Its solutions are not just about protection but also about empowering businesses with insights and tools to manage threats proactively, making Hornetsecurity a preferred choice for those seeking to fortify their email environments against sophisticated social engineering attacks.

Source: Hornetsecurity Demo, July 2024

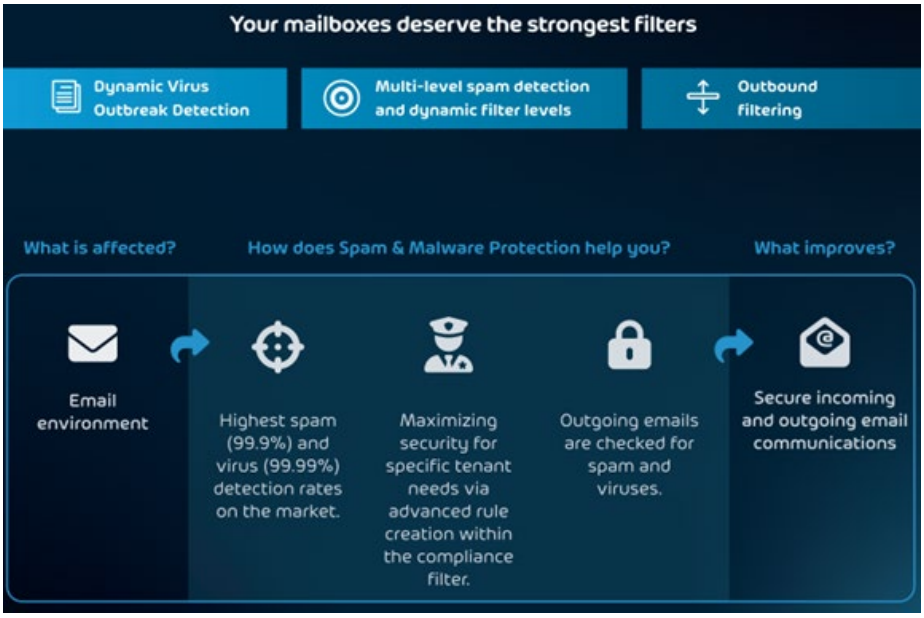
Social Graph Capabilities

Hornetsecurity has developed a sophisticated social graph system that maps out all interactions between users within an email environment. It captures metrics like frequency of communication, whether it's a first interaction or not, and additional metadata such as location. The primary aim of this feature is to detect and flag any unusual communication patterns or unexpected new inputs into the social graph. When such anomalies are detected, actions like quarantining messages or rerouting them to specific folders via ICES are automatically initiated.

Currently, this social graph functionality is backend driven, but there are plans for a user interface where one can visualize the social graph, navigate through it, and configure specific security actions based on the insights gained from the graph. This

interface is expected to be rolled out later in the year, enhancing user interaction with this security feature.

Moreover, Hornetsecurity's approach with the social graph extends its utility beyond just email security into creating a scalable infrastructure for message processing with advanced policy enforcement. This technology not only serves Hornetsecurity's direct customers but also integrates into solutions for OEMs and service providers, where the vast data collected enhances threat intelligence and supports features like safe unsubscribe from newsletters, as seen with the integration with Cisco's products. This safe unsubscribe feature leverages AI to dynamically interact with web pages, ensuring all necessary fields are correctly filled to complete the unsubscribe process, even adapting to changes in web page layout over time.



Source: Spam and Malware Protection, Hornetsecurity website, 2024

Threat Intelligence Capabilities

Hornetsecurity is evolving its email security product from merely protective measures to comprehensive threat management, effectively turning it into a mini security operations center (SoC) for email. This evolution allows managed service providers (MSPs) to leverage these insights when offering their services by providing visibility into user interactions with emails, including how users report and respond to threats in real time.

Regarding threat intelligence feeds:

- **Default Threat Intelligence Feeds:** Hornetsecurity primarily uses its own threat intelligence data within the product, which is derived from its extensive network of email filtering operations across various customers and partners.
- **Integration of External Feeds:** Currently, there is limited support for ingesting external threat intelligence feeds directly into its system for individual customers. Hornetsecurity itself can choose to buy and integrate external feeds, but this is not a standard feature open to all customers. For instance, Hornetsecurity might use URL feeds not to directly ingest the data but rather to enhance its own scanning processes, where it confirms the threat before adding it to their system.
- **Purpose of External Feeds:** When external feeds are used, it's often to supplement data from regions where Hornetsecurity might not have as much direct collection through its partnerships with telecoms, thus enhancing the global coverage of their threat intelligence. To guarantee an extremely low false positive rate, Hornetsecurity is extremely cautious about implementing external feeds. Any use of external feed is always conditioned by automated AI qualification before injecting the data.

This approach underscores Hornetsecurity's cautious stance on integrating external threat intelligence, prioritizing the quality and reliability of threat data to ensure that it does not compromise the integrity of its system with potentially inaccurate or outdated information. However, my conversation with Hornetsecurity hints

at a potential flexibility to adapt based on specific customer needs or strategic partnerships, indicating that, while not standard, customized solutions might be possible under certain conditions or for specific customers.

Technology Highlights

1. **Computer Vision and AI:**

- **Usage:** Hornetsecurity's technology includes computer vision for analyzing emails and web pages to identify phishing attempts. This includes:
  - **Logo Recognition:** Detecting and analyzing logos to identify phishing, even when logos are slightly altered or recreated using modern techniques like pixel art via HTML tables.
  - **Phishing Evolution:** Adrien noted the increasing sophistication of phishing tactics where logos are modified just enough to bypass traditional hash-based detection methods. Computer vision helps in recognizing these subtle changes.
- **AI Engine Training:** For detecting BEC, AI models are trained using data augmentation due to the scarcity of real-world samples. This involves creating synthetic data to simulate various BEC scenarios for better model training.

2. **QR Code Security:**

- **Detailed Process:**
  - **First Analysis:** Initial assessment to identify QR codes based on image characteristics.
  - **Second Analysis:** Computer vision deciphers the QR code to extract the URL, followed by a comprehensive analysis of the linked web page for threats.
- **Resource Management:** Given the resource-intensive nature of computer vision, there's an emphasis on efficient deployment:
  - **Post-Delivery Actions:** Due to possible delays in processing, the system includes an autoremediate function:

- **Action Customization:** Upon detection of a threat, options include moving the email to a different folder, deleting it, or adding a warning banner to the message.
- **Retroactive Remediation:** If a threat is detected after delivery, the email solution can retroactively remove or flag the email directly from the user's mailbox.

3. **Hybrid Deployment Model:**

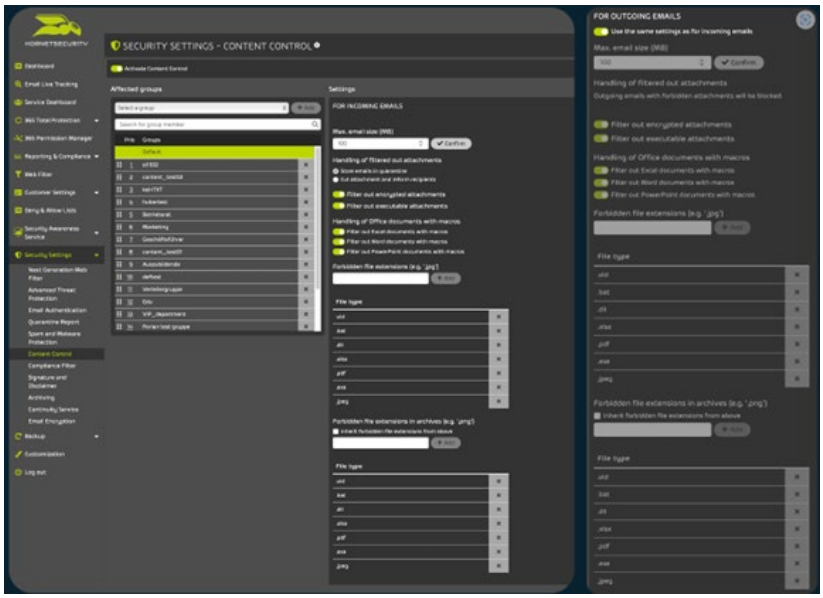
- **Flexibility:** Allows integration into existing infrastructures either inline or via API, providing both pre- and post-delivery security measures. Hornetsecurity calls this its hybrid mode and allows customers to choose between mail exchanger (MX) DNS record updates (secure email gateway; SEG) pure API (ICES), or hybrid for a robust, layered security approach.
- This model is integrated into Hornetsecurity products, enhancing deployment options and management.

4. **AI Recipient Validation:**

- **Social Graph Utilization:** Uses the established communication patterns within an organization to prevent sensitive information from being sent to unintended recipients, thus reducing errors and enhancing security. In my opinion this was on par with Proofpoint's recent Tessian acquisition that offers similar capabilities.

5. **Permission Manager for Collaboration Tools:**

- **Control Over Permissions:** Manages access rights for Microsoft 365 tools, automatically adjusting permissions like expiring anonymous links to prevent unauthorized access. This functionality gives CISOs a more comprehensive view of permissions and whether items are shared with others, helping them to better protect sensitive information. It allows Microsoft 365 admins to define compliance policies for sharing sites, files, and folders in Microsoft 365 and then easily monitor the states of policy compliance and audit policy violations – which helps organizations maintain compliance with internal and external regulations and policies.



Source: Spam and Malware Protection, Hornetsecurity website, 2024

Sources

Spam and Malware Protection – Hornetsecurity – Next-Gen Microsoft 365 Security

Hornetsecurity Analyst Briefing, July 2024

Our Take

With its innovative security solutions, Hornetsecurity offers a comprehensive suite of tools designed to combat the sophisticated landscape of cyber threats. Its technical prowess shines through features like advanced phishing detection with computer vision, AI-driven recipient validation, and a flexible hybrid deployment model that caters to a wide array of customer needs, from cloud SEG to ICES integrations. This flexibility not only simplifies integration into existing IT infrastructures but also enhances security without compromising performance.

What sets Hornetsecurity apart is not just its technology but its global reach and the expertise of its staff. With worldwide deployment, Hornetsecurity ensures that its solutions are not only scalable but also culturally and regionally adaptive, providing robust security for organizations regardless of their location. The knowledgeable team behind Hornetsecurity continuously innovates to support next-generation threats like ATO, VEC, and BEC, leveraging their deep understanding of social engineering tactics to refine their defenses.

By integrating its data-centric approach with its commitment to cutting-edge security, Hornetsecurity offers a holistic security solution that not only detects but also predicts and mitigates sophisticated email-based attacks. This synergy of technology, expertise, and global presence establishes Hornetsecurity as a formidable player in safeguarding digital communication against ever-evolving threats.

Source: Hornetsecurity Demo, July 2024

About Info-Tech Research Group: Info-Tech Research Group is one of the world's leading research and advisory firms, proudly serving over 30,000 IT and HR professionals. The company produces unbiased, highly relevant research and provides advisory services to help leaders make strategic, timely, and well-informed decisions. For nearly 30 years, Info-Tech has partnered closely with teams to provide them with everything they need, from actionable tools to analyst guidance, ensuring they deliver measurable results for their organizations.

To learn more about Info-Tech's divisions, visit McLean & Company for HR research and advisory services and SoftwareReviews for software buying insights.