Kingston: A Case Study in API Security Transformation with Salt

Real-world results are seen from Salt Security deployment

- Blocked six attacker IPs based on Salt's initial API risk discovery within two weeks of deployment
- Salt enabled Kingston to roll out an effective API posture governance program to mitigate potential posture gaps.
- Rapid integration with Cloudflare Worker collector and CloudFlare WAF to block advanced API threats

Kingston is a multinational American computer technology corporation that develops, manufactures, sells, and supports flash memory and other computer-related memory products. Kingston faced a common challenge in today's digital landscape: unprotected and potentially unknown APIs that could expose sensitive data and create an expanded attack surface. Before Salt, Kingston lacked complete visibility into their API ecosystem, exposing them to potential breaches and compliance concerns. As APIs and microservices became more mainstream and widely used in Kingston, a new approach was needed for security, a dilemma faced by many CISOs and CIOs across many organizations.

The Turning Point: Embracing API Security with Salt

Kingston achieved a paradigm shift in their security posture by implementing the Salt API Security Platform. Here's how Salt addressed their key challenges:

> Salt has been a game-changer for our API security. We now have the visibility and control to protect our data, stay compliant, and build trust with our customers. We're confident that Salt will remain a valuable partner as we navigate the ever-evolving threat landscape.

Peter Rios
Infrastructure and Information Security Manager, CISM

- Visibility into the Hidden: Salt provided unprecedented visibility into Kingston's sanctioned and unsanctioned APIs. This critical insight allowed them to shrink their attack surface and prioritize API protection efforts.
- Pinpointing Sensitive Data: Salt's advanced capabilities pinpointed sensitive data exposures within APIs, enabling Kingston to strengthen data security and comply with regulations like CCPA, GDPR, PCI, and ISO 270001.
- Proactive Protection: Salt's runtime protection features integrate with and go beyond traditional WAFs to help safeguard against slow and low-level attacks and ensure alignment with the OWASP API Top 10.
- Actionable Insights: Salt's posture gap analysis identified non-compliance with internal security standards, guiding Kingston's remediation efforts and continuously improving API security.

Beyond Security: The Business Impact

While the security benefits are undeniable, Salt's impact extends beyond technical measures:

- Increased Confidence: Having their APIs secured, Kingston gained increased confidence in their products and services, potentially leading to higher customer trust and retention.
- Streamlined Processes: Salt's automated security checks and incident response capabilities reduced reliance on manual audits, potentially optimizing resource allocation and reducing operational costs.

Looking Ahead: A Continuous Journey

Kingston's journey with Salt is ongoing. They plan to:

- Utilize Salt's open API to connect with their DAST solution, further strengthening their security posture.
- Expand Salt deployment to additional platforms like Citrix ADC, ensuring comprehensive API protection across their infrastructure.

- Kingston's digital transformation will continue at scale, and with the Salt Platform in place, they will be assured that any potential risks will be detected and remediated rapidly.

Conclusion:

Kingston's story is a testament to the power of Salt's Security Platform. The Salt Platform allowed Kingston complete visibility into its API posture and was quickly able to highlight risk while working seamlessly with its existing security stack. By proactively addressing potential API security risks, Kingston transformed its security posture, enhanced its business operations, and paved the way for continued success in a digital world increasingly driven by APIs.