FORTINET ACQUIRES ENSILO

To enhance the value of our Security Fabric offering and meet evolving requirements and facilitate additional growth, we announced on October 28, 2019, the acquisition of enSilo, a leading provider of advanced endpoint security solution that offers a broad Endpoint Protection Platform (EPP) combined with Endpoint Detection and Response (EDR) capabilities.

Organizations are concerned about succumbing to the threat landscape, ransomware and data theft that cause significant business disruption.   Most organizations find threat detection and response more difficult today than two years ago. And the security operation centers (SOCs) face challenges in ensuring network and data security if they have many disparate solutions that are not tightly integrated to work together effectively.

The combination of Fortinet and enSilo addresses those challenges for enterprise and service providers of all sizes by delivering automated protection against advanced threats, pre- and post-execution, with sophisticated integrated threat prevention and orchestrated incident response functionality.

KEY QUESTIONS

Q: How does enSilo enrich Fortinet's security offerings?

A: enSilo has a strong team of talented technical professionals who have built a great product. The enSilo product enhances the value of Security Fabric by adding real-time detection, protection, and response enhancements to further protect endpoints and corresponding edge data. Fortinet intends to offer customers additional security effectiveness through the integration of enSilo's endpoint detection and response (EDR) technology with Fortinet's FortiSIEM solution, FortiInsight UEBA (user entity behavior analytics) features, and FortiNAC solution.

Enterprises will benefit from superior endpoint visibility and tightly coordinated, dynamic control of network, user, and host activity within their environment. Service Providers can also benefit by providing value-add services or managed detection and response (MDR) services from the broad, integrated Fortinet platform that will now include advanced EDR.

Q: What market problem does this acquisition address?

A: The acquisition of enSilo addresses the enterprise security leaders' concerns of advanced threats, cyber security skill shortage and business availability.

1) Advanced threats/ Ransomware - enterprises security leaders are worried about succumbing to the advanced threat landscape – i.e. data theft and Ransomware. They also realize that 100% prevention is not realistic, and even enterprises with the best security need robust detection and response. enSilo stops data breaches in real-time, and its patented code-tracing technology further enables incident investigation and response.

2) Skill shortage - Enterprises often have challenges in recruiting and retaining enough security expertise in-house. Traditional EDR tools are heavy and noisy, with so many false positives that they can be counter-productive to security and cause alert fatigue. The products of these traditional players in the market are not only expensive to operate but also require a very specific skillset.   enSilo provides automated threat detection, containment and response that helps eliminate false positives and dwell time and provides full attack chain visibility and automates much of the tracking and response functionality. Furthermore, enSilo's team of cyber security experts offers advanced forensics services.

3) Business availability - Keeping the digital business up and running 24x7 is an imperative. As such, in many cases organizations cannot upgrade all systems without downtime, and patching is still a challenge. Further, they won't want to reboot systems to remediate incidents. Unlike most EPP/EDR vendors Ensilo is unique in not only

mitigating vulnerabilities with virtual patching but also enabling selective remediation without impacting business continuity.

Q: Can you explain enSilo technology or product offerings?

A: enSilo is a next-gen endpoint security solution that packs a broad set of EDR capabilities, and is easy to deploy and use. enSilo offers certified NGAV, automated EDR, threat hunting, forensics and virtual patching capabilities all in one single agent to prevent breaches and comply with regulations like PCI/DSS and HIPAA. The agent is lightweight (less than 1% of CPU, 60MB RAM) and is managed by an easy-to-use management console for pre and post-infection capabilities. enSilo features multi-tenant management in the cloud, on-premise, and hybrid.

Q. Will the enSilo product become part of the Fortinet brand?

A. Yes.

Q: How will enSilo be integrated into Fortinet Security Fabric?

A. As an existing Fabric-ready partner, enSilo already complements FortiGate Firewalls, FortiSandbox, and FortiClient Fabric Agent. We plan to deliver additional native integrations with multiple Fabric solutions as well.

Q: Where is enSilo located?

A: enSilo is headquartered in San Francisco California, with an office in Israel.

Q: Who are enSilo's customers?

A: Mid- to large enterprises across multiple vertical industries and service providers whose security leaders are concerned primarily about data breach, and data loss caused by advanced attacks or ransomware attacks. While enSilo's solution is sold broadly across verticals, some key ones include manufacturing, retail and hospitality, financial services. Moreover, enSilo's ability to detect, contain and remediate threats without causing downtime is a key reason for success inOT/critical infrastructure environments that require high availability.

In retail and hospitality sectors where majority of the point of sale (POS) solutions and other embedded systems are still running on older Windows platforms (XP) and have limited system resources, enSilo's light footprint (under 60 MB) and the ability to run on legacy Windows is a key differentiator.

State and local governments concerned about ransomware attacks deploy enSilo to protect their data.

For industry specific information and case studies: https://www.ensilo.com/resources/#case-studies

Q: What are the benefits to Fortinet partners of this acquisition?

A: Partners will benefit from this acquisition in a number of ways, including selling an expanded product and services portfolio that enrich partners' security offering and add value for end user customers with integrated solutions for advanced threat protection, SOC optimization, IoT and Edge security. Adding enSilo to our Security Fabric significantly increases the addressable market and the ability to up-level their strategic sales conversations with CISOs.
Service Providers will be able to extract the full value of this combination and deliver a comprehensive and efficient managed detection and response (MDR) service, leveraging the native cloud infrastructure and multitenancy as a foundation for the security service practices.

Q: Will the enSilo products be sold via the existing Fortinet Channel?

A: Yes. Consistent with our standard business practices we will ensure channel is also trained and enabled to sell this exceptional solution both as a standalone and with our Fabric products, a few of which are already integrated with enSilo.

Q: What does this mean for Fabric Ready Partners?

A: The openness of the Fortinet Security Fabric ensures that we integrate seamlessly with Fortinet competitive and non-competitive products. In the same way that we have Endpoint Security Fabric Ready Partners even while offering our own Endpoint Security Product (FortiClient), we will continue to partner with companies in this space.