

<b>FOR ADVANCED EMAIL</b> Email security platform for inbound and outbound threat protection with unmatched effectiveness	<b>FOR SECURITY ORCHESTRATION AND RESPONSE</b> Better Infrastructure & Resources to Identify & Mitigate Threats	<b>FOR COMPLIANCE</b> Avoid fines, and reduce compliance costs	<b>FOR DIGITAL RISK</b> Protect your business and customers from Web, Social Media, and Mobile apps fraud
<b>Email Protection (EP)</b> Stop advanced threats (malware, phishing, and fraud) before they get to people while improving productivity. Filter, classify and manage unwanted email – including spam, bulk, and impostor (BEC). EP has robust reporting and search, as well as flexible deployment options (cloud, on premises).	<b>Threat Response</b> Improve your cybersecurity operational efficiency and better allocate resources while maximizing your ROI. Orchestrate, automate and accelerate your incident response. Automatically confirm incident infections, enrich alerts, and enable automatic or push of a button containment. Out-of-the-box multi-vendor solution.	<b>Enterprise Archive</b> Available for email, files, social media, IM and custom applications, archive in the cloud for compliance, supervision and legal discovery. Double Blind Encryption a patented technology, allows organizations to retain exclusive access to their data while outsourcing it. Full search and discovery capabilities.	<b>Domain Discover</b> Protect your organization, partners, vendors, and customers from email fraud, targeted malware, and phishing campaigns by persistently monitoring, finding and taking down fraudulent, lookalike, unauthorized web domains.
<b>Targeted Attack Protection (TAP)</b> More than 90% of targeted attacks start through email so improve your security posture; get visibility into the threats entering your organization and protect against targeted attacks that use malicious attachments and URLs. Get detailed forensics to speed up your incident response, and see who is attacking, how they're attacking, and what they're after. Links can be poisoned after delivery or threats are missed, in those cases, TAP will also let you know what threats were missed and who was affected.	<b>Data Discover</b> Reduce your attack surface and compliance risk by finding exposed sensitive or confidential data sitting on a network shared drive, or SharePoint sites, and enable real-time remediation through quarantine, access revocation or deletion. Cloud architecture makes deployment fast and easy, and policy is integrated across data at rest, email (Email DLP), and cloud (SaaS Protection).	<b>Enterprise Collaboration Archiving</b> FINRA and SEC regulations require all electronic communications (sent or received) to be archived. Fines are stiff. Capture social posts (associated links and attachments) for all, or a subset, of users from Salesforce, Chatter, Jive, Skype for business, LinkedIn, Twitter, and Facebook, and store them into your existing information archive. Specify your internal journaling email address, and we handle the rest. Robust reporting, social conversations can be grouped similar to email replies.	<b>Social Patrol</b> Protect and monitor your branded social media accounts ensuring positive customer experience and compliance. Detect takeovers, lock down compromised accounts, monitor, and remove malicious, inappropriate or non-compliant content and control connected applications. Using natural language processing (not a word bank) for enforcement, it integrates directly with social platforms, publishing tools, and other security solutions like Palo Alto Networks and Splunk.
<b>Threat Response Auto Pull</b> Limit further damage, by automating and accelerating your email incident response process. Threat Response Auto Pull delivers automatic or push-button capability to quarantine delivered malicious email even if forwarded or sent to a distribution list. Save countless hours of searching and scripting while mitigating risk.	<b>Mobile Defense</b> Reduce your Bring Your Own Device policy risk while protecting employee privacy. We will scan official and secondary app stores, analyze apps code, behavior, and dynamic operating attributes and provide visibility into apps that pose a high-security risk. Combining rich mobile app analysis (50M+ Android and iOS threat database), with automated workflows that orchestrate deployed MDMs, EMMs or MSMS, Mobile Defense safeguards organizations from data exfiltration and fraud.	<b>Compliance Gateway</b> Ensure that your content is properly retained with a built in feedback loop to confirm successful message delivery and automated or manual resubmission. Route content to multiple destinations (archives, supervision or analytic systems) based on policy. Can process any content type delivered through SMTP (email, instant messaging, and social media). Supported downstream archives include HP-Autonomy, Data minder and our Enterprise Archive.	<b>Social Syndicate</b> Balance compliance and speed. Make it easier to collect, review and syndicate content to your social media properties with little publishing flow disruption. A single platform that channels publishing requests and provides supervision workflows powered by automated security, compliance, and acceptable use checks. Automatically discover malware, inappropriate language, and simple mistakes before they go live.
<b>Email Fraud Defense (EFD)</b> Protect your business, brand, and supply chain from Email Fraud. Authenticate legitimate e-mail and by extension block fraudulent activity using your domains with superior visibility and efficacy. Global visibility, comprehensive intelligence, and managed services model make it easy and safe to authenticate all your legitimate senders with DMARC and block fraud.	<b>ET Intelligence</b> Knowing your adversary and having insight into their tactics, techniques, and procedures is paramount when conducting cyber hunting activities. Access hourly updated, 100% verified threat intelligence with context and history. ET Intelligence has proof of conviction, 40+ threat categories, five-year history, and samples, as well as related domains and IPs.	<b>E-discovery and Analytics</b> Expedite early case assessments (ECA) and improve your litigation readiness strategy. Search millions of messages in seconds, empower legal teams with self-serve tools, slash review time by 90% with in-house tools, reduce third party costs by minimizing exports, improve insight and decision making with advanced analytics and visualizations.	<b>Social Discover</b> Protect your brand and customers. Find fraudulent associated social media accounts using persistent and automated account searches, and content auditing, across all the leading networks: Facebook, Youtube, Twitter, Google +, Instagram, and LinkedIn.
Avoid compliance violations and loss of competitive edge by securing protected, confidential, or trade secret info. <b>Email Data Loss Prevention (DLP)</b> Prevent negligence with accuracy and control. <b>Email Encryption</b> Automatically encrypt outbound email messages and attachments.	<b>SaaS Protection</b> Deploy Office 365, G Suite, and Salesforce with confidence. Automate policy-based response actions to alert or restrict access to content based on its sensitivity (PII, PHI) or user's risk (ex: a user has been exposed to phishing or malware, or has logged in from different geographies in a short period). Prevent malware uploads (ex: word file with URL link to credential phish site) and control third party add-ons.	<b>Intelligent Supervision</b> Review teams spend too much time searching for violations; allow them to sift through data to meet FINRA, SEC, IIROC and other needs. Intelligent Supervision makes reviewers more efficient by creating "less noise" in fulfilling supervision obligations, i.e it shows violations previews, offers sampling by message type (skip bulk emails) and conversation threading grouping related messages. Export full history of review activities to auditors.	<b>Social Sight</b> Organizations encouraging employees to promote their brand in social networks need to secure employee's social media accounts without sacrificing their privacy. Only employee advocacy program that provides insight into security, acceptable use, and compliance risks while maintaining 100% employee control over their accounts and privacy. Opt-in model with easy deployment.
<b>Continuity</b> When people's routine work flows are interrupted, their productivity drops. Avoid internal, and customer communication disruptions, especially for cloud email services like O365. Send and receive email and access contacts and calendar items anytime, anywhere, and from any device.	<b>Targeted Attack Protection SaaS Defense</b> SaaS applications are a security blind spot for most enterprises. Detect malicious files in Google Drive, OneDrive, SharePoint, and Box, find users affected and gain visibility into the size, scope, and type of threats you face with the same world class detection leveraged in TAP for email.	<b>Social Patrol and Social Syndicate</b> Descriptions under Digital Risk.	<b>Mobile Discover</b> Protect your brand and customers. Locate fraudulent, lookalike, unauthorized mobile apps that put your brand and customers at risk. Also, find legitimate outdated app versions that remain available to download or are hosted on third-party stores without your permission.