

Proofpoint beveiligt samenwerking en data in nieuwe agentic werkomgeving

Nieuwe oplossingen als AI-tools en slimme agents laten organisaties AI gebruiken terwijl ze onverwachte risico's omzeilen

Amsterdam, 23 September 2025 – [Proofpoint, Inc.](#), een toonaangevend cybersecurity- en compliancebedrijf, kondigt vandaag vier nieuwe innovaties aan voor de samenwerking tussen mens en AI-agents, [ontwikkeld voor de beveiliging van de agentic werkomgeving](#). Proofpoint's nieuwe samenwerkings- en datasecuritymogelijkheden pakken de fundamentele risico's van de agentic werkomgeving aan door vier grote uitdagingen op te lossen: het beschermen van AI-assistenten tegen gerichte aanvallen, zorgen voor de correcte controles ter voorkoming van dataverlies door mensen en agents, het beheren van de acties van GenAI en AI-agents en het gebruik van AI-agents om samenwerking en datasecurity voor securityprofessionals te automatiseren.

Net zoals digitale transformatie de digitale werkomgeving heeft gecreëerd, doet AI dit voor de agentic werkomgeving. AI-agents en -assistants werken samen met mensen om meer productiviteit mogelijk te maken. Toch vergroten ze ook het aanvalsoppervlak in een ongekend tempo.

AI-agents en -assistants worden steeds vaker geïntegreerd in workflows, waar ze taken automatiseren. Ook analyseren ze informatie en werken ze samen met zowel mensen als met elkaar. Deze agents zijn zo ontworpen dat ze zich gedragen als mensen. Ze klikken, delen en handelen. Dat betekent dat ze ook kunnen worden misleid, bedrogen, of gecompromitteerd. Mensen en agents lopen tegen vergelijkbare risico's aan. Van social en prompt engineeringaanvallen, tot het onbevoegd openbaar maken van gevoelige data en inloggegevens. Daarom hebben ze vergelijkbare en uitgebreide bescherming nodig.

“De agentic werkomgeving is een realiteit en vormt een van de meest fundamentele veranderingen waarop werk wordt uitgevoerd”, zegt Sumit Dhawan, CEO bij Proofpoint. “Het beschermen van de agentic werkomgeving is de volgende stap van human centric security. Dit gaat verder dan alleen mensen, want het moet de AI-agents, de punten waar zij samenwerken en data delen, beschermen. Het is ons doel om ervoor te zorgen dat onze klanten met vertrouwen AI kunnen gebruiken. Zij doen dit, wetende dat wij zowel hen als hun data beschermen tegen nieuwe dreigingen.”

De vier innovaties die Proofpoint vandaag aankondigt, zijn ontworpen om de agentic werkomgeving veilig te maken. Deze innovaties beveiligen dat waar mensen, agents en data met elkaar in verbinding staan.

- **Opsporen en voorkomen van AI-exploits via e-mail: mensen en agents in staat stellen te vertrouwen op samenwerking in de agentic werkomgeving**
Aanvallers plaatsen steeds vaker kwaadaardige prompts in e-mails om AI-assistants, zoals Microsoft Copilot en Google Gemini, te manipuleren. Deze bewapende berichten maken gebruik van promptinjecties om kwaadaardige informatie naar de eindgebruiker te sturen. Ook verwarren ze op AI-gebaseerde verdedigingsmechanismen en exfiltreren ze gevoelige data. [De nieuwe](#)

[technologieën van Proofpoint](#), geleverd via de Proofpoint Prime Threat Protection oplossing, blokkeren deze exploits nog voordat ze de inbox bereiken. Zo kunnen mensen en AI-agents elke interactie vertrouwen.

- **Proofpoint Data Security Complete en Proofpoint AI Data Governance: uniforme datasecurity met AI-databeheer**

Data is in de tijd van AI de snelst groeiende bron van securityrisico's geworden. De nieuwe oplossing van Proofpoint, [Proofpoint Data Security Complete](#), zorgt dat organisaties hun gevoelige data kunnen lokaliseren, correct classificeren en bepalen wie er toegang toe heeft. Ook monitort het hoe mensen ermee omgaan via alle kanalen, via eindpunten en e-mail tot het web en de cloud. In tegenstelling tot andere oplossingen biedt Proofpoint Data Security Complete detectie en classificatie via Autonomous Custom Classifiers. Deze verzorgen een nauwkeurigere, dynamische en robuuste dataclassificatie, met minimale menselijke input. De oplossing creëert ook een datarisico-overzicht (inclusief cross-channel dataherkomst en de identificatie van configuratie-, toegangs- en exfiltratierisico's) en biedt oplossingen met één druk op de knop. Het biedt een diepgaande integratie van DSPM, DLP, insider threat management en data lineage in één oplossing.

Proofpoint AI Data Governance stelt organisaties in staat om zowel goedgekeurd als onbevoegd AI-gebruik te ontdekken en vooraf opgestelde beleidsregels toe te passen om exfiltratie en privacyschending te voorkomen. Ook beheert het toegang met geautomatiseerde workflows voor securityteams en contenteigenaren.

- **Proofpoint Secure Agent Gateway: voorkomen dat door klanten geïmplementeerde AI-agents data verliezen**

In de agentic werkomgeving wordt gevoelige data niet langer alleen door mensen verwerkt. AI-agents, gebouwd en geïmplementeerd door organisaties, hebben ook toegang tot waardevolle data en gesprekken. Deze vereisen hetzelfde beschermingsniveau als hun menselijke tegenhangers. [Proofpoint Secure Access Gateway](#) is gebouwd met behulp van Model Context Protocol (MCP). Het controleert hoe AI-agents toegang krijgen tot data, monitort de activiteiten van agents, dwingt beleid voor datagebruik af en blokkeert gevoelige data voordat het gedeeld wordt met mensen of andere agents. Proofpoint Secure Agent Gateway werkt samen met het Proofpoint Data Security Complete-aanbod om de eerste oplossing in de branche te bieden voor het beveiligen van data voor zowel mensen als agents.

- **Proofpoint Satori™ Agents en Proofpoint Satori™ MCP Access: een kracht voor securityteams**

[Proofpoint Satori™ Agents](#) werken binnen Proofpoint-oplossingen. Ze voeren taken uit zoals het afhandelen van data loss prevention waarschuwingen en het aanraden van phishing-simulaties. Ook lossen ze het door gebruikers gemelde e-maildreigingen voor ondernemingen die het Proofpoint-platform gebruiken op. Met Proofpoint Satori Agents kunnen teams die Proofpoint-oplossingen beheren, securityoperaties stroomlijnen en schalen, tijdrovende repetitieve taken elimineren en waarschuwingsvermoeidheid verminderen. Ook zet het data inzichten om in automatische acties.

Met Proofpoint Satori™ MCP Access kunnen andere agents, zoals CrowdStrike Charlotte en Microsoft Copilot, Proofpoint Satori Agents raadplegen om tussen platformen samen te werken, securityactiviteiten te versnellen, repetitieve taken te automatiseren en betere securityresultaten te behalen. Proofpoint Satori MCP Access gebruikt het Model Context Protocol (MCP) om Proofpoint eenvoudig te integreren met andere securityoplossingen.

“De opkomst van de agentic werkomgeving verandert cybersecurity fundamenteel”, zegt Ryan Kalember, Chief Strategy Officer bij Proofpoint. “Door samenwerking en datasecurity te combineren, zorgen we voor een nieuwe manier waarop organisaties hun werk beveiligen in het tijdperk van AI. Proofpoint is de eerste die een oplossing biedt waarmee organisaties kunnen achterhalen waar hun data zich bevindt, begrijpen wat deze data is en beschermen wat zowel mensen als agents ermee doen. Hiermee hebben zij het vertrouwen om te innoveren, samen te werken en veilig te schalen met AI, geïntegreerd in hun meest cruciale workflows.”

Beschikbaarheid

De nieuwe mogelijkheden die vandaag zijn aangekondigd, worden de komende maanden op het Proofpoint-platform geïntroduceerd. AI-exploitedetectie via e-mail wordt naar verwachting in het vierde kwartaal van 2025 geïntroduceerd. Proofpoint Data Security Complete is vanaf dit kwartaal (Q3-2025) beschikbaar. In de komende twee kwartalen worden nieuwe functies toegevoegd. Proofpoint Secure Agent Gateway en Proofpoint Satori Agents zijn vanaf 2026 gefaseerd beschikbaar.

Over Proofpoint, Inc.

Proofpoint, Inc. is een wereldwijde leider op het gebied van human-centric en AI-agent centric cybersecurity, die ervoor zorgen dat mensen, data en AI-agents veilig met elkaar communiceren via e-mail, cloud en samenwerkingstools. Proofpoint is een vertrouwde partner van meer dan 80 Fortune 100-bedrijven, meer dan 10.000 grote ondernemingen en miljoenen kleine organisaties bij het stoppen van dreigingen, het voorkomen van dataverlies en het opbouwen van veerkracht bij mensen en AI-workflows. Het samenwerkings- en datasecurityplatform van Proofpoint helpt organisaties van elke omvang hun mensen te beschermen en te versterken, terwijl ze AI veilig en vol vertrouwen omarmen. Meer informatie op www.proofpoint.com.

Volg Proofpoint op [LinkedIn](#)

Proofpoint is een geregistreerd handelsmerk of handelsnaam van Proofpoint, Inc. in de Verenigde Staten en/of andere landen. Alle andere handelsmerken in dit document zijn eigendom van hun respectieve eigenaren.