dotforce
Your Source for Innovative Cybertech

Portfolio tecnologico

Aprile 2020

Web Application Security
Web Vulnerability Management

Acunetix Web Vulnerability Scanner effettua scansioni automatiche su siti web standard e personalizzati, identificando le vulnerabilità delle applicazioni verso attacchi di tipo SQL Injection, XSS (Cross-Site Scripting), XXE, SSRF, Host Header e scoprendo altri 500 tipi diversi di vulnerabilità. Il prodotto è disponibile sia in modalità On Premise (Acunetix Standard e Premium) sia in versione On Premise / Cloud (Acunetix360).

- **Acunetix Standard** è uno scanner di vulnerabilità del web, che testa automaticamente il tuo sito Web per vedere se può essere hackerato. Lo scanner esegue in modo sicuro attacchi simulati, mostra come un hacker malintenzionato potrebbe potenzialmente accedere ai tuoi sistemi e spiega come prevenire attacchi reali. Questo è il modo migliore per proteggerti dalle comuni minacce web.

- **Acunetix Premium** si rivolge principalmente alle organizzazioni medio-grandi che devono proteggere un gran numero di siti e applicazioni Web, o che desiderano incorporare la Web Security nelle loro DevOps.

- **Acunetix 360** è una soluzione Cloud-based di Web Vulnerability Assessment & Management, progettata per far parte di qualsiasi ambiente aziendale fornendo integrazioni multiple e opzioni per l'integrazione in contesti personalizzati. E' disponibile anche On Premise (Linux-based)

Acunetix è un leader globale per la web security. Prima società a realizzare uno scanner di vulnerabilità web totalmente dedicato e automatizzato, Acunetix porta sul campo un'esperienza senza rivali. Acunetix web vulnerability scanner è utilizzato con fiducia da clienti che operano in ambienti con elevate necessità di sicurezza, tra cui numerose aziende Fortune 500.

Secure Email Cloud

Ci sono più di quattro miliardi di caselle di posta elettronica nel mondo. Milioni di utenti inviano e ricevono centinaia di miliardi di messaggi ogni giorno. I cybercriminali ne approfittano, trasformando quelle che dovrebbero essere comunicazioni affidabili in uno strumento grazie al quale possono rubare dati sensibili e generare profitti. Agari combatte questi criminali informatici con una missione audace: proteggere le comunicazioni digitali per garantire che l'umanità prevalga sul male.

- **Agari Phishing Defense™**
  Ferma minacce sofisticate di identity deception tra cui BEC (business email compromise), executive spoofing, e account takeover.

- **Agari Phishing Response™**
  Accelera il triage di episodi di phishing, e l'attività di forensics, remediation, breach containment per i Security Operations Center (SOC).

- **Agari Brand Protection™**
  Automatizza l'autenticazione e l'enforcement delle e-mail con DMARC, per prevenire gli abusi dei brand aziendali, proteggendo i clienti da costosi e insidiosi attacchi email.

Agari Identity Graph™
Agari Identity Graph è un database grafico ad alte prestazioni di relazioni e modelli comportamentali tra individui, marchi, aziende, servizi e domini che utilizza centinaia di caratteristiche per definire comunicazioni affidabili.

Agari utilizza l'AI predittiva per modellare l'identità su scala Internet e prevenire il prossimo attacco zero-day. Concentrandosi sull'identità del mittente e sul comportamento rispetto al tipo di attacco stesso, Agari modella il buono per proteggerti dal male, assicurando che nessuna minaccia, nuova o esistente, arrivi nella tua casella di posta.

Centrify Privileged Access Management	Da più di dieci anni Centrify è riconosciuta come società leader nel mercato **PAM (Privileged Access Management)**. Basandosi su queste solide fondamenta, Centrify eleva la propria tecnologia PAM a livelli ancora più alti grazie ai servizi Zero Privilege, pronti per il cloud, riducendo e rendendo più sicura la superficie di attacco delle aziende moderne. **Zero Trust Privilege** ridefinisce il concetto di Privileged Access Management (PAM) adattandolo alle superfici a rischio delle imprese moderne. Le organizzazioni devono scartare il vecchio modello di "fiducia ma verifica", che si basava su confini ben definiti. Zero Trust impone un approccio "non fidarti mai, verifica sempre, garantisci i privilegi minimi necessari" all'accesso privilegiato, dall'interno o dall'esterno della rete. **Centrify Privileged Access Service** - Concessione dell'accesso agli account privilegiati tramite un account condiviso, password o password applicazioni e vault segreti, nonché protezione dell'accesso remoto. Accesso amministrativo sicuro tramite jump box, richieste di accesso e approvazioni basate sul flusso di lavoro, nonché autenticazione a più fattori (MFA) presso il Vault. L'approccio Zero Trust Privilege è basato sulla verifica di chi richiede l'accesso, sul contesto della richiesta e sul rischio dell'ambiente di accesso. Implementando l'accesso con privilegi minimi, le organizzazioni riducono la superficie di attacco, migliorano la visibilità di audit e conformità e riducono rischi, complessità e costi. Oggi, oltre 5.000 imprese in tutto il mondo, tra cui metà delle Fortune 50 e oltre 80 agenzie federali, si affidano a Centrify.

corero DDoS Mitigation	Corero Network Security si dedica al miglioramento della sicurezza e della disponibilità di Internet, attraverso lo sviluppo di soluzioni innovative di mitigazione DDoS. E' un'azienda eader nella protezione dagli attacchi DDoS automatici in tempo reale ad alte prestazioni, con visibilità, analisi e reportistica completi degli attacchi. Le soluzioni sono di tipo On Premise, Cloud oppure ibride, e proteggono migliaia di organizzazioni che operano in diverse tipologie di settore merceologico in tutto il mondo. La famiglia di soluzioni Corero SmartWall® Threat Defense System (TDS) utilizza la moderna architettura di mitigazione DDoS per rimuovere automaticamente e chirurgicamente il traffico di attacchi DDoS, consentendo allo stesso tempo in modo ininterrotto il flusso legittimo di traffico di rete verso gli utenti.

DOMAINTOOLS Threat Intelligence & Hunting, WHOIS	**DomainTools** aiuta gli analisti della sicurezza a trasformare i dati delle minacce in informazioni. La soluzione utilizza gli indicatori di rete, compresi domini e IP, collegandoli con quasi tutti i domini attivi su Internet. Queste connessioni informano le valutazioni dei rischi, aiutano a profilare gli aggressori, guidano le indagini sulle frodi online e mappano l'attività di cyber sull'infrastruttura degli attaccanti. L'obiettivo è fermare le minacce alla sicurezza delle aziende prima che si verifichino, utilizzando dati dominio/DNS, analisi predittiva e monitoraggio delle tendenze su Internet. Vengono raccolti dati OSINT (Open Source Intelligence) da molte fonti, insieme a record storici, in un database centrale. I dati sono analizzati in base a vari algoritmi di connessione per fornire informazioni utili, tra cui il punteggio del dominio e la mappatura legale. DomainTools ha oltre 10 miliardi di punti di dati DNS correlati per costruire una mappa di "chi sta facendo cosa" su Internet. Le aziende Fortune 1000, le agenzie governative globali e i principali fornitori di soluzioni per la sicurezza utilizzano DomainTools come strumento critico nel loro lavoro di indagine e mitigazione delle minacce.

Real Time IT analytics
Network Traffic Security
Network Performance

La rete è l'unica cosa che collega tutte le interazioni digitali. ExtraHop ha inventato un modo radicalmente nuovo per osservare e analizzare queste interazioni: l'elaborazione del traffico di rete in tempo reale, che è una fonte di informazioni completa, unica e affidabile per il business, la sicurezza e l'IT.

ExtraHop offre visibilità in tempo reale su tutta l'azienda ibrida, traffico cloud e crittografato compreso. ExtraHop trasforma i raw wire data in informazioni strutturate, mentre l'apprendimento automatico consente di scoprire e rispondere a minacce nascoste, con impatto zero sulle prestazioni.

ExtraHop è progettato per soddisfare le esigenze di scalabilità dell'impresa ibrida moderna, dal Core al Cloud. La piattaforma Reveal(x) trasforma la rete in una fonte di sicurezza e visibilità IT più completa e oggettiva, fornendo al tempo stesso un ricco set di dati – wire data – che permette un apprendimento automatico focalizzato, preciso e affidabile come nessun altro.

Visibilità senza precedenti: l'analisi in tempo reale consente di rilevare e classificare tutte le risorse aziendali, mappare tutte le connessioni e le dipendenze e monitorare il flusso di traffico fino a 100 Gbps (incluse le sessioni crittografate SSL o PFS).

Approfondimenti precisi: l'apprendimento automatico avanzato utilizza rivelatori potenti basati sulla riduzione della dimensionalità e sul rilevamento di valori anomali per identificare le anomalie, correlando tali dati con le risorse critiche per far emergere le minacce incombenti.

Risposte immediate: Un semplice flusso di lavoro di tipo investigativo stabilisce una causa inequivocabile in pochi secondi (e non giorni), mentre le integrazioni aziendali accelerano e automatizzano la risposta prima che le minacce incidano sulla tua attività.

ExtraHop Reveal(x) fornisce il rilevamento e la risposta della rete nativa del cloud per l'impresa ibrida. Il nostro approccio innovativo analizza tutte le interazioni di rete e applica l'apprendimento automatico su scala cloud per visibilità completa, rilevamento in tempo reale e risposta intelligente. Con questo approccio, aiutiamo le principali aziende mondiali a superare il rumore di allarmi, silos organizzativi e tecnologia in fuga.

Indipendentemente dal fatto che tu stia investigando sugli attacchi, assicurando la disponibilità di applicazioni critiche o proteggendo i tuoi investimenti nel cloud, ExtraHop ti aiuta a rilevare le minacce fino al 95% più velocemente e a rispondere del 60% in modo più efficiente.

ExtraHop è progettato per soddisfare le mutevoli esigenze e la solida scalabilità dell'impresa ibrida moderna, dal Core al Cloud. La piattaforma Reveal(x) trasforma la rete in una fonte di sicurezza e visibilità IT più completa e oggettiva, fornendo al tempo stesso un ricco set di dati – wire data – che permette un apprendimento automatico focalizzato, preciso e affidabile come nessun altro.

Multilayer Endpoint Protection	Fondata nel 1996, Faronics ha sede a Vancouver, nella Columbia Britannica ed è una società privata con quasi 30.000 clienti che utilizzano oltre nove milioni di licenze in oltre 150 paesi. Faronics produce software che consente di gestire, semplificare e proteggere gli ambienti di elaborazione multiutente. La suite di prodotti Faronics garantisce la disponibilità al 100% di ogni workstation e libera i team IT dai problemi legati al supporto tecnico del software. Di casa negli ambienti Education con Deep Freeze, Faronics è un vendor molto apprezzato anche in ambito Enterprise. • Faronics Deep Freeze riduce i costi IT preservando le configurazioni ideali dei computer su cui viene implementato. • Faronics Anti-Executable impedisce l'utilizzo di software non autorizzato • Faronics Anti-Virus garantisce protezione dal malware. • Faronics Power Save aiuta a ridurre i costi energetici. • Faronics Insight offre il controllo totale sui computer delle aule informatiche, e • Faronics WINSelect consente agli amministratori IT di personalizzare l'accesso alle applicazioni, a siti web, programmi e opzioni di Windows.
Identity & Access Management Single Sign On Adaptive Authentication	Viviamo in una nuova era. Ci aspettiamo che tutto sia disponibile in ogni momento e in ogni luogo. L'ambiente composto da API, servizi cloud, dispositivi e dati che guidano questa trasformazione è estremamente complesso. Le aziende espandono le risorse e i team IT aldilà delle loro location fisiche, e le identità diventano il nuovo perimetro di sicurezza. Allo stesso tempo, la sofisticazione e la portata delle violazioni che minacciano questo nuovo mondo non hanno precedenti. Siamo letteralmente sotto assedio. Nessuna azienda è immune e sono in poche a essere al passo con i tempi. Questo nuovo scenario richiede un nuovo tipo di piattaforma di accesso. Nato da Centrify e basato su Zero Trust, Idaptive sta creando una nuova era – accesso sicuro ovunque – che integra perfettamente SSO, MFA, EMM e UBA, e rende più forti le difese di sicurezza aziendale, gestendo e mettendo al sicuro le identità dalle minacce cyber.
Threat Response Platform Intrusion Detection & Prevention	LookingGlass Cyber Solutions offre una protezione unificata dalle minacce contro sofisticati attacchi informatici alle imprese globali e alle agenzie governative, rendendo operativa l'intelligence sulle minacce attraverso il suo portafoglio end-to-end. Le piattaforme di intelligence delle minacce scalabili e i prodotti di risposta alle minacce basati sulla rete utilizzano i nostri feed di dati leggibili automaticamente per fornire una sicurezza completa basata sulle minacce. L'aumento del portafoglio di soluzioni è un team mondiale di analisti della sicurezza che arricchisce continuamente i nostri feed di dati e offre ai clienti capacità di comprensione e risposta senza precedenti nei rischi informatici, fisici e di terze parti. Approfondimenti prioritari, pertinenti e tempestivi consentono ai clienti di agire sull'intelligence delle minacce attraverso le diverse fasi del ciclo di vita degli attacchi. LookingGlass **Aeonik Security Fabric**, un'architettura di sicurezza completa, definita dal software, costruita appositamente per soddisfare le esigenze degli ambienti di rete sempre più senza confini ed elastici di oggi. Un approccio fondamentalmente nuovo alla sicurezza informatica, Aeonik è un sistema di rilevamento e prevenzione delle intrusioni di nuova generazione (IDPS) che illumina tutte le aree della rete per identificare, cacciare, interrompere e rispondere rapidamente alle attività avversarie al momento e al punto di attacco.

netwrix **Auditing, Governance, GDPR**	Netwrix Auditor è una piattaforma di visibilità e di governance che permette il controllo su modifiche, configurazioni e l'accesso in ambienti IT di cloud ibrido, per proteggere i dati indipendentemente dalla loro posizione. A differenza di software di controllo IT tradizionale, la piattaforma fornisce analisi di sicurezza per rilevare anomalie nel comportamento degli utenti e indagare i modelli di minaccia prima che si verifichi una violazione dei dati. Netwrix Auditor è in grado di rilevare minacce alla sicurezza dei dati fornendo analisi di sicurezza sui cambiamenti critici, le configurazioni e l'accesso ai dati stessi.

onelogin **Identity & Access Management**	Il passaggio al cloud offre risparmi, infrastrutture ridotte e migliore usabilità. Ma anche un'azienda ibrida presenta delle sfide: la frammentazione dell'IT mentre le organizzazioni cercano di gestire le app in ambienti cloud locali e multipli. L'approccio più diffuso richiede più sistemi **IAM (Identity Access Management)** per diversi ambienti, reti e dispositivi, portando con sé ancora più problemi: maggiore complessità e costi più elevati per l'IT, un'esperienza utente insoddisfacente e un maggiore rischio per la sicurezza. Adesso c'è un modo migliore. La piattaforma **OneLogin UAM (Unified Access Management)** centralizza l'accesso all'interno della tua organizzazione e soddisfa le esigenze in rapida evoluzione della tua azienda ibrida. Ti offre sicurezza, affidabilità e controllo per tutti i tuoi dati, dispositivi e utenti. Entrambi i fondatori di OneLogin, Thomas e Christian Pedersen, sono stati coinvolti nel successo della migliore applicazione di help desk on-demand al mondo: Zendesk. Attraverso le loro interazioni con i clienti di Zendesk, è diventato evidente ai fondatori che le aziende si stavano muovendo nel cloud a frotte. Mentre il cloud computing offre numerosi vantaggi, la gestione di dozzine di applicazioni cloud pone sfide significative in termini di sicurezza e produttività. L'idea è nata per creare una soluzione di gestione dell'identità e degli accessi facile da usare come le applicazioni cloud da cui le aziende dipendono. OneLogin è stato lanciato nella primavera del 2010 e ha ricevuto il supporto di CRV. Da allora, OneLogin ha collaborato con i principali fornitori SaaS e ha ottenuto la fiducia delle organizzazioni attente alla sicurezza in tutto il mondo.

perimeter 81 Software Defined Perimeter VPN Alternative	**Perimeter 81** è la seconda iniziativa lanciata nel 2018 da due esperti di sicurezza informatica come Amit Bareket e Sagi Gidali. Incontratisi all'Università di Tel Aviv nel 2012, hanno unito le loro forze per fondare SaferVPN, che ora è uno dei marchi VPN più conosciuti al mondo e recentemente è stato acquisito da un conglomerato leader di Internet e dei media. Fin dalla sua fondazione, Perimeter 81 ha rapidamente guadagnato terreno nel mercato del perimetro della rete come servizio definito dal software (Software-Defined Perimeter) e come **alternativa sicura alle tradizionali VPN**, e sta trasformando il modo in cui le aziende consumano la sicurezza della rete. Perimeter 81 è stato nominato Gartner Cool Vendor, ha vinto numerosi premi per la sicurezza informatica e detiene un brevetto per la sicurezza Wi-Fi automatica. La società sta trasformando il mondo dell'accesso sicuro alla rete e aiutando le aziende di tutti i settori e dimensioni a spostarsi in modo sicuro nel cloud e potenziare la loro forza lavoro moderna e mobile. Il team di esperti Perimeter 81 si riunisce ogni giorno per offrire un servizio SaaS veramente innovativo e creare uno sportello unico per le offerte di sicurezza informatica.

Plixer Network Traffic Analysis	Plixer fornisce un sistema di analisi del traffico di rete che supporta la risposta agli incidenti rapida ed efficiente. La soluzione consente di ottenere visibilità sulle applicazioni cloud, sugli eventi di sicurezza e sul traffico di rete. Fornisce dati utilizzabili per guidare l'utente dal rilevamento di eventi di rete e di sicurezza fino all'analisi e alla mitigazione delle cause principali. Gli incidenti di rete e di sicurezza sono inevitabili. Quando si verificano, Plixer è lì per aiutarti a tornare rapidamente alla normalità e ridurre al minimo l'interruzione dell'attività. Migliaia di organizzazioni si affidano alle soluzioni Plixer per mantenere efficiente l'infrastruttura IT. **Scrutinizer** Scrutinizer, il sistema di analisi del traffico di rete di Plixer, raccoglie, analizza, visualizza e genera report sui dati di ogni conversazione di rete e transazione digitale per fornire sicurezza e informazioni di rete. Fornisce le informazioni dettagliate e storiche necessarie per gestire e ottimizzare le operazioni aziendali, riducendo al contempo i rischi rilevando e correggendo gli incidenti. **FlowPro** Le sonde FlowPro supportano la gestione delle prestazioni delle applicazioni e le funzionalità di difesa per il monitoraggio del traffico DNS. Da una singola sonda, le operazioni di rete possono gestire e ottimizzare la rete in modo efficiente, mentre le operazioni di sicurezza sono in grado di ridurre contemporaneamente i rischi, acquisire il contesto dei dati e rispondere rapidamente agli incidenti di sicurezza. **Replicator** Replicator aggrega, replica e distribuisce i metadati di flusso e log esportati dalla rete esistente su più strumenti di monitoraggio come SIEM, syslog e flow collector. Ciò migliora il valore dei dati semplificando notevolmente aggiunte, spostamenti e modifiche e proteggendo la CPU dall'esportazione di switch, router, firewall, ecc.

RAPID7 Vulnerability Management, AppSec, SIEM, SOAR	Rapid7 è un fornitore leader di soluzioni di dati e analisi di sicurezza che consentono alle organizzazioni di implementare un approccio attivo e orientato all'analisi alla sicurezza informatica. La piattaforma di dati e analisi di sicurezza è stata creata appositamente per affrontare e gestire al meglio un ambiente IT sempre più complesso e caotico. Rapid7 combina una vasta esperienza in dati e analisi di sicurezza con una profonda conoscenza dei comportamenti e delle tecniche degli aggressori, per dare un senso alla ricchezza di dati a disposizione delle organizzazioni sui loro ambienti IT e utenti. Le analisi potenti e proprietarie consentono alle organizzazioni di contestualizzare e stabilire la priorità delle minacce che si trovano ad affrontare le loro risorse fisiche, virtuali e cloud, comprese quelle poste dai comportamenti dei loro utenti. Sfruttando la piattaforma di dati e analisi di sicurezza, le soluzioni Rapid7 consentono alle organizzazioni di gestire in modo strategico e dinamico la loro esposizione alla sicurezza informatica. Le nostre soluzioni consentono alle organizzazioni di prevenire gli attacchi fornendo visibilità sulle vulnerabilità e per rilevare rapidamente i compromessi, rispondere alle violazioni e correggere le cause di fondo degli attacchi.

securosys Hardware Security Modules	Securosys SA è stata fondata da Andreas Curiger e Robert Rogenmoser all'inizio del 2014. La società sviluppa, produce e distribuisce hardware, software e servizi che proteggono e verificano i dati e la loro trasmissione. I prodotti sono sviluppati e costruiti in Svizzera e con partner certificati in Europa. L'azienda dà grande importanza alla propria filiera sicura di approvvigionamento. Non ci sono backdoor. Per garantire la massima trasparenza, i clienti Securosys possono esaminare tutti i blueprint e il codice sorgente. I prodotti principali di Securosys sono gli Hardware Security Module (HSM) della serie Primus. Primus HSM è disponibile come box dedicato o come servizio cloud. Il portafoglio di offerta dell'azienda si completa con Centurion Network Encryptor per creare reti completamente crittografate.

Siemplify Next-Gen SOAR Platform	Siemplify nasce dall'esigenza di un modo migliore, più semplice ed efficace per gestire le operazioni di sicurezza. La soluzione è stata costruita daesperti delle operazioni di sicurezza che hanno trascorso anni ad affinare le loro capacità in prima linea nelle agenzie israeliane di cibernetica. I fondatori di Siemplify – Amos Stern, Alon Cohen e Garry Fatakhov – hanno aggiunto a questa esperienza una costante attività di formazione e di miglioramento dei team SOC in tutto il mondo. Il loro background approfondito nella gestione SOC, analisi della sicurezza e scienza dei dati, unito alla conoscenza diretta delle sfide quotidiane dei team di operazioni di sicurezza, ha portato alla creazione della Siemplify Security Operations Platform, la piattaforma indipendente leader del settore SOAR.
stealthbits Data Access & AD Governance	STEALTHbits è un'azienda produttrice di software per la sicurezza dei dati. Si focalizza sulla sicurezza delle informazioni aziendali, difendendole dagli abusi delle credenziali e controllando l'accesso ai dati. L'azienda propone tre soluzioni principali: StealthAUDIT – Auditing, compliance, e framework di governance per dati non strutturati e applicazioni critiche; StealthINTERCEPT – Identificazione delle minacce in tempo reale, change monitoring e alerting per infrastrutture Microsoft; StealthDEFEND – Soluzione di analisi del comportamento degli utenti e di identificazione delle minacce.
STRONGKEY Encryption, Strong Authentication, Key Management	StrongKey, Inc. è una società privata con sede a Silicon Valley, in California. È leader nell'infrastruttura di gestione delle chiavi di livello enterprise, portando nuovi livelli di capacità e sicurezza dei dati a un prezzo decisamente inferiore rispetto alle altre soluzioni presenti sul mercato. Fornendo prodotti e servizi nella gestione delle chiavi simmetriche, crittografia, tokenizzazione e PKI, StrongKey si concentra sulla protezione dei dati nel cloud computing, nell'e-commerce, nella sanità, nella finanza e in altri settori che richiedono la protezione dei dati sensibili. StrongKey ha definito un'architettura per applicazioni Web unica, conforme al Regulatory Cloud Computing (RC3), che consente il cloud computing sicuro. L'architettura RC3 è stata convalidata dai clienti per la protezione dei dati finanziari e sanitari utilizzando le soluzioni di StrongKey.
TitanHQ SpamTitan AntiSpam Gateway Cloud & VA	L'email è senza dubbio la principale applicazione utilizzata da ogni azienda oggi per comunicare, inviare e condividere informazioni. Tuttavia, le email "buone" rappresentano meno del 5% di tutto il volume delle email inviate e ricevute ogni giorno. Il 95% è spam. Servono strumenti antispam scalabili, robusti e accurati per gestire questo problema (di sicurezza, ma anche di prestazioni che vengono ridotte da questo enorme volume di traffico), e tutto ad un prezzo che riesca ad adattarsi al grande numero di utenti che supportano. Con Clienti in oltre 100 paesi nel mondo, SpamTitan è una delle soluzioni antispam più complete sul mercato per proteggere gli utenti dallo spam e dalle minacce che si trasmettono e propagano via email. SpamTitan utilizza tecnologia allo stato dell'arte per offrire una soluzione facile da implementare e da gestire, ma dalle elevate caratteristiche e funzionalità di sicurezza. La versione On Premise (SpamTitan Gateway) permette di creare una propria email gateway appliance, fisica (ISO) o virtuale (Virtual Machine), offrendo protezione da Virus, Spam, Malware, Phishing e altro contenuto indesiderato. La versione Cloud non necessita di infrastruttura locale, e unisce la sicurezza di SpamTitan alla flessibilità del Cloud. SpamTitan nasce per domini illimitati, ed è quindi ideale per Internet Service Provider che desiderino offrire un servizio AntiSpam affidabile ai loro Clienti.

TitanHQ WebTitan **Web Filtering** **Gateway, Cloud & WiFi**	WebTitan è una soluzione di **web content filtering** avanzata, in grado di offrire protezione da minacce alla sicurezza che si diffondono via HTTP e HTTPS, e controllo evoluto sul **protocollo DNS** per la sicurezza di aziende, organizzazioni educational e Managed Service Provider. Premiata con cinque stelle da SC Magazine, permette alle aziende di proteggere i propri dati ed i propri utenti da malware e altre minacce Internet come virus, spyware, e phishing, e allo stesso tempo, offre strumenti di limitazione e controllo per rendere efficace l'attuazione delle politiche aziendali che riguardano la navigazione Internet. La soluzione è disponibile in modalità On Premise e Cloud. La versione Cloud non necessita di infrastruttura locale, e unisce la sicurezza di WebTitan alla flessibilità del Cloud. **WebTitan for WiFi** permette di implementare il web content filtering sugli Access Point predisposti dai WiFi Service Provider.

yubico **Multifactor Authentication** **FIDO2, WebAuthn**	Yubico è stata fondata in Svezia nel 2007 con la missione di rendere il login sicuro facile e disponibile per tutti. Nel 2011, Stina, CEO e fondatore e Jakob, CTO, si sono trasferiti nella Silicon Valley per realizzare il sogno. In stretta collaborazione con le principali società di Internet e leader di pensiero, è stato creato il supporto nativo per le YubiKey nelle principali piattaforme e browser online, consentendo una connessione Internet più sicura per miliardi di persone. Oggi, il team Yubico è situato in 7 paesi e le Yubikey, prodotte in Svezia e negli Stati Uniti, hanno conquistato la fiducia delle più grandi imprese e milioni di utenti in tutto il mondo. Yubico cambia le regole del gioco per la strong authentication, offrendo sicurezza di livello superiore insieme a una facilità di utilizzo ineguagliata. Il prodotto principale, la YubiKey, è un piccolo dispositivo USB e NFC che supporta numerosi protocolli crittografici e di autenticazione e che garantisce l'accesso a qualsiasi numero di sistemi IT e servizi online. Con un semplice tocco, la YubiKey protegge l'accesso a computer, reti e servizi online per le più grandi organizzazioni del mondo. Yubico crea standard universali come principale contributore al protocollo aperto di autenticazione a due fattori FIDO Universal. La tecnologia Yubico è apprezzata da milioni di utenti in oltre 160 nazioni. Per proteggere i segreti sui server, Yubico ha creato anche YubiHSM, il modulo di sicurezza hardware più piccolo al mondo. L'azienda offre agli sviluppatori server open source, supporto e servizi di validazione in hosting per una facile integrazione con qualsiasi sistema IT.

ZEROFOX **Digital Risk & Brand Protection**	ZeroFOX, leader nel mercato della protezione digitale e sui social media, protegge le aziende di oggi dai rischi fisici, oltre che inerenti il marchio e la sicurezza dinamica, su piattaforme social, mobile, web e di collaborazione. Mediante l'utilizzo di varie origini dati e dell'analisi basata sull'intelligenza artificiale, la piattaforma ZeroFOX Platform identifica e risolve gli attacchi di phishing mirati, la compromissione delle credenziali, la fuga di dati, l'utilizzo non autorizzato del marchio, le minacce agli executive e relative alla posizione, e molto altro ancora. La tecnologia SaaS brevettata ZeroFOX elabora e protegge giornalmente milioni di post, messaggi e account nel panorama digitale e dei social media, compresi LinkedIn, Facebook, Slack, Twitter, HipChat, Instagram, Pastebin, YouTube, App Store mobili, deep e dark web, domini …

dotforce
Your Source for Innovative Cybertech

Via S. Anna 41 | 20090 Vimodrone (MI) | Tel. 02/36735520 | Fax 02/36215698 | www.dotforce.it | info@dotforce.it