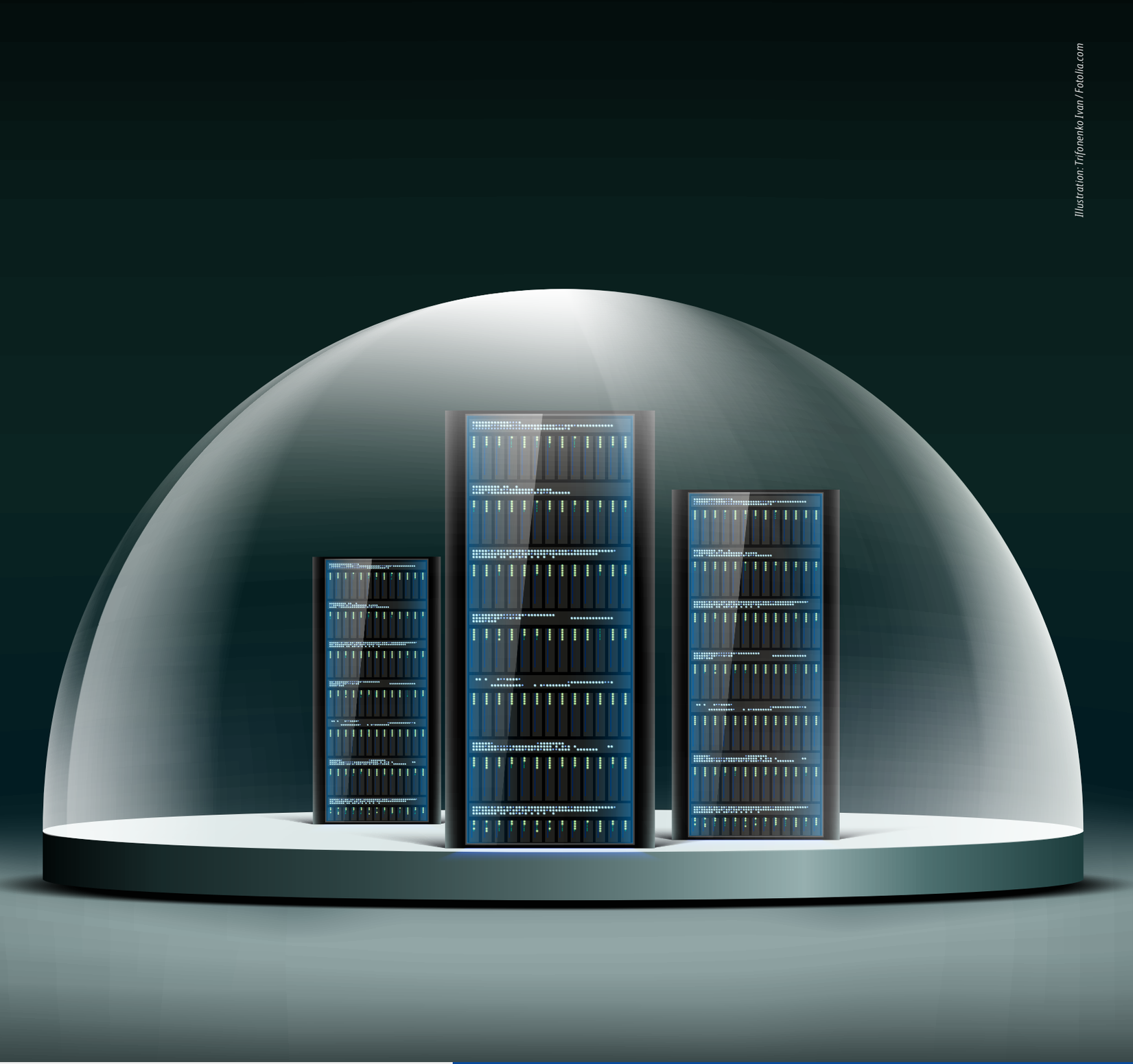


Illustration: Trifonenko Ivan / Fotolia.com

Dossier
Cybersecurity

In Kooperation mit **Boll Engineering**

Ein virtueller Schutzschild gegen Attacken aus dem Internet

osc. Internet und E-Mail sind Einfallstore für alle möglichen Bedrohungen der IT-Systeme einer Firma. Ransomware, Trojaner oder Phishing-Versuche – sowohl Anzahl als auch Raffinesse der Attacken aus dem Cyberspace nehmen laufend zu. Auf der anderen Seite arbeiten Cybersecurity-Anbieter unermüdlich an Wegen, Unternehmen vor den digitalen Gefahren zu schützen.
Eine Antwort auf der Suche nach mehr Sicherheit im Netz lautet «Isolation». Der Nutzer eines Browsers soll dabei von den eigentlichen Inhalten aus dem Web isoliert werden. Websites oder E-Mails werden – samt eventuell vorhandenem Schadcode – zunächst in einer virtuellen Umgebung ausgeführt und dann als «schädlingsfreie» Version ohne Scripts oder Flash-Inhalte an den Nutzer weitergeleitet, versprechen die Hersteller. Wie das funktioniert, erklären Patrick Michel und Roger Gomringer von Boll Engineering auf den folgenden Seiten.

Mit «Isolation» gegen Cybergefahren

Zero-Day- und Drive-by-Attacken werden von konventionellen Sicherheitslösungen nicht erkannt und können dramatische Folgen haben. Dank «Isolation» der User vor schädlichen Inhalten ist es nun möglich, derartige Angriffe vollständig abzuwehren – ohne Einbussen hinsichtlich Geschwindigkeit und User-Komfort.

DER AUTOR

Patrick Michel,
Head of Sales, Boll Engineering

Die Gefahren aus dem Cyberspace nehmen rasant zu. Die Angriffe werden raffinierter und komplexer – und sie sind allgegenwärtig, wie dem aktuellen «State of the Web Report» eines Anbieters von Sicherheitslösungen zu entnehmen ist. Demnach wurden 44 Prozent der Top-100 000-Websites des «Alexa-Rankings» als riskant eingestuft. Dies weil sie entweder Malware verbreiten oder kürzlich gehackt wurden oder weil sie unsichere Software nutzen.

Neben dem Besuch riskanter Websites sind auch ausgeklügelte Phishing-Attacken ein grosser Gefahrenherd. Sie zielen mittels persönlicher Ansprache und empfängerbezogener Details präzise auf den einzelnen Adressaten – man spricht von «Spear Phishing» – und nutzen zur Verbreitung oft bekannte, populäre Dienste wie News- und Reise-Websites. Die Analysten von Gartner bezeichnen das Internet mit all seinen Diensten mittlerweile als «Kloake von Attacken».

Erkennung reicht nicht

Herkömmliche Cybersicherheitsarchitekturen setzen auf das Prinzip «Detection». Dabei erkennen Anti-Malware-Lösungen bekannte Malware-Muster und versetzen die betroffenen Inhalte in Quarantäne. Zudem blockieren sogenannte Webfilter auf Basis von Blacklists den Zugang zu gefährlichen Websites.

Auch Sandboxing basiert auf Schadcode-Erkennung. Dabei wird der zu prüfende Code in einer geschützten Umgebung ausgeführt und anhand des Verhaltens als gefährlich oder nicht gefährlich eingestuft.

Security und Business stecken in einem Dilemma.

So verbreitet die auf Detection basierende Cyberabwehr auch sein mag: sie ist nur begrenzt ein probates Mittel, um unbekannte Angriffsmethoden, sogenannte Zero-Day-Attacken, abzuwehren. Deutlich wurde dies mit dem Aufkommen von Ransomware, von der unzählige Nutzer trotz Einsatz ausgeklügelter Anti-Malware-Lösungen betroffen sind. Darüber hinaus hat eine rein erkennungsbasierte Cyberabwehr einen weiteren Nachteil: Sie sperrt nicht nur den Schadcode, sondern kann auch die Produktivität der Mitarbeitenden negativ beeinflussen. So können die User beispielsweise nur noch eingeschränkt im Web surfen, da in manchen Unternehmen selbst anerkannte Medien- und Social-Media-Angebote gesperrt sind. Die Sperrung einzelner Websites erfolgt nicht ohne Grund, wie diverse Vorfälle auch in der Schweiz zeigen. So wurde über 20minuten.ch im April 2016 Schadcode per Drive-by-Infection verteilt – eine eingebettete Anzeige eines Werbenetzwerks war mit einer Malware-Site verlinkt. Angesichts der grossen Zahl von Scripts und Dritt-Websites, von denen Inhalte geladen werden, ist dies nicht erstaunlich. Untersucht man die Startseite des genannten Mediums, stösst man beispielsweise auf 93 Scripts und 25 Background-Sites. Das sind durchaus typische Werte für Online-Newsplattformen.

Eine Isolationsplattform nimmt Webinhalte entgegen und führt sämtlichen aktiven Code wie Javascript und Flash in einer abgeschotteten virtuellen Umgebung aus.

Generell lässt sich sagen, dass Security und Business in einem Dilemma stecken. Einerseits wird alles potenziell Gefährliche auf die Webfilter-Blacklist gesetzt. Andererseits wollen die Fachabteilungen einen möglichst freien Zugang zum Web, um in ihrer Arbeit nicht behindert zu werden. Doch zu berücksichtigen ist, dass die zunehmende Verflechtung von Websites dazu führt, dass heute eigentlich keiner Site mehr vertraut werden kann. Deshalb ist aus Security-Sicht das Webfiltering nur noch begrenzt nützlich. Sicherheitsrelevante Webfilter-Kategorien decken nur noch einen Bruchteil der gefährlichen Sites ab, und das Blockieren von einzelnen Websites oder von anderen Website-Kategorien beeinträchtigt die Produktivität der Mitarbeitenden im Übermass.

«Isolation» bringt starke Abwehr

«It's time to isolate» postulierte Gartner schon 2016. Die Idee dahinter: Anstatt den Zugang zu bestimmten Inhalten komplett zu blockieren, wird der Empfänger vom direkten Zugang zum Web isoliert und erhält ausschliesslich gefahrlose Website-Inhalte, E-Mails und Dokumente. Somit übernimmt eine Instanz zwischen User und gefährlicher Website den risikoreichen Job.

Auf dem Markt finden sich bereits erste isolationsbasierte Security-Lösungen. Einige davon setzen schlicht auf eine Virtual-Desktop-Infrastruktur. Dabei werden die Originalinhalte in einer zentralen virtuellen Umgebung abgerufen und verarbeitet – an das Gerät des Nutzers wird nur ein Videostream übermittelt. Dadurch ist die Sicherheit zwar gewährleistet, aber der Nutzerkomfort ist beeinträchtigt. Zudem sind VDI-basierte Lösungen aufwendig

und bringen markante Zusatzkosten mit sich. Andere Lösungen platzieren die virtuelle Umgebung direkt auf dem Endgerät. Wirklich praktikabel ist dies nicht: Wenn auf jedem Mitarbeiter-PC eine virtuelle Maschine oder Browser-Instanz laufen soll, nehmen die Hardwareanforderungen und der Administrationsaufwand zu. Zudem sind entsprechende Lösungen auf einzelne Browser und Betriebssysteme limitiert.

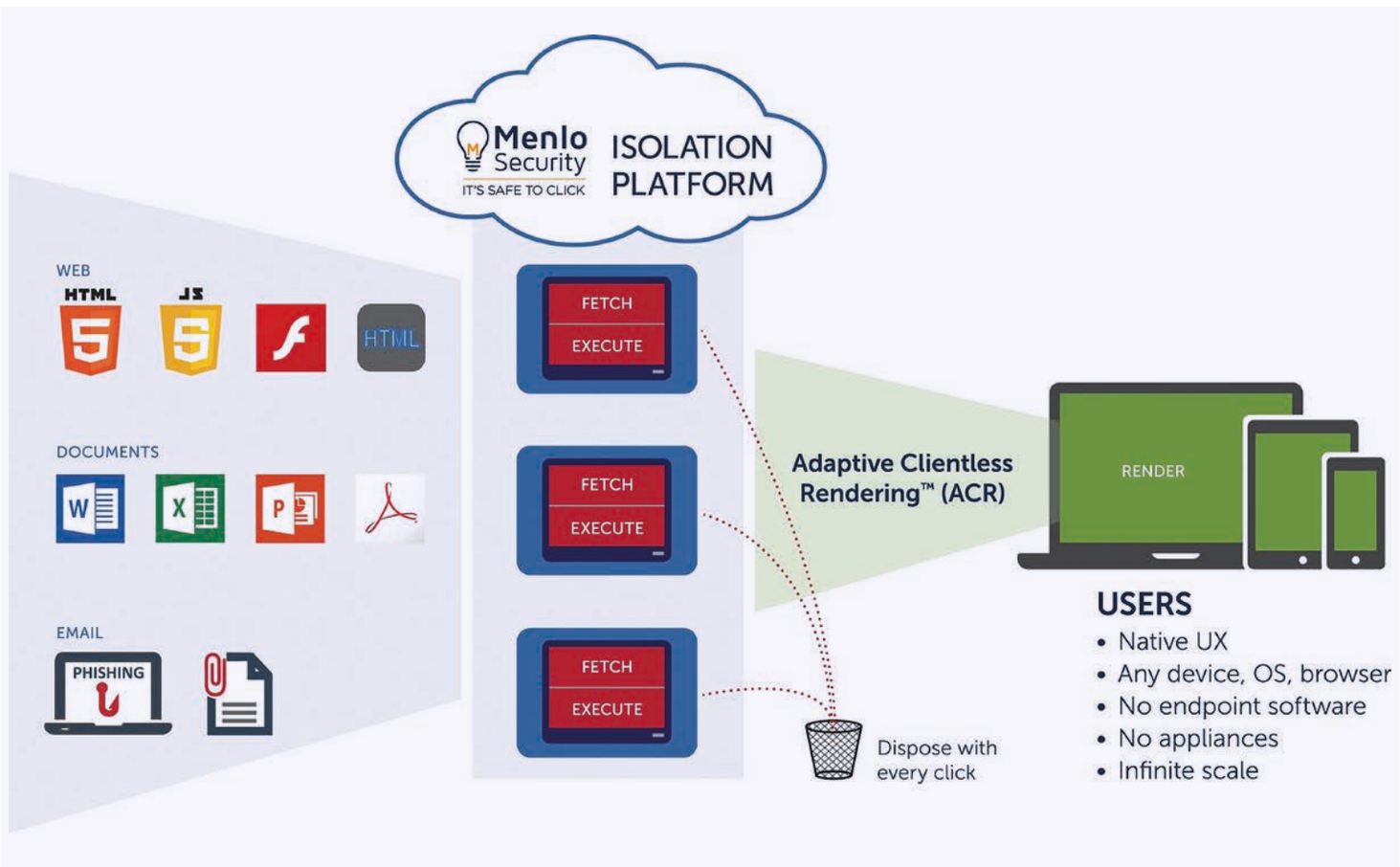
Die ideale Isolationsplattform

Um eine ideale Kombination von vollständiger Isolation, hohem Nutzerkomfort und geringem Administrationsaufwand zu erreichen, ist eine Architektur erforderlich, die inhärent auf «Native User Experience», Ressourceneffizienz und enterprisetaugliche Skalierbarkeit ausgelegt ist – so wie dies im folgenden Beispiel illustriert wird.

Eine auf dem Markt erhältliche Isolationsplattform nimmt Webinhalte entgegen und führt sämtlichen aktiven Code wie Javascript und Flash in einer abgeschotteten virtuellen Umgebung aus. Eine mögliche Infektion findet zwar statt – dies jedoch in einem «Käfig», aus dem sie nicht ausbrechen kann. Die ursprünglichen Inhalte werden sofort nach der Ausführung «entsorgt». Der Nutzer beziehungsweise dessen Endgerät erhält eine gerenderte, von aktivem Code befreite Version. Scripts wurden entfernt, Flash-Videos automatisch ins MP4-Format umgewandelt. Dieses clevere Prinzip lässt sich nicht nur für Webinhalte, sondern auch für Dokumente und E-Mails einsetzen. So werden empfangene Dokumente in der abgeschotteten Umgebung analysiert und als sichere Vorschau ohne aktiven Inhalt weitergeleitet. Auf eigenes Risiko kann der Nutzer auch die Originalversion herunterladen. Zudem werden E-Mails auf gefährliche Links untersucht und durch einen sicheren Link ersetzt, der auf die Isolationsplattform zeigt.

Bei der beschriebenen Isolationsplattform muss auf dem Endgerät keine Client-Software installiert werden – der Nutzer arbeitet mit dem üblichen Browser und Mail-Client mit gewohntem Komfort. Und er kann alle Features nutzen. Auch die Einrichtung ist einfach: Die Isolationsplattform liefert die gerenderten Inhalte über einen Proxy-Service aus. Auf dem Endgerät muss dazu nur eine Proxy-Einstellung konfiguriert werden. In einer gemanagten Umgebung ist dies über eine Konfigurations-URL zentral gesteuert möglich. Die Isolationsplattform lässt sich zudem zusammen mit bestehenden Proxy-, Firewall- und Webfilter-Lösungen einsetzen und ergänzt diese um eine zusätzliche Sicherheitsstufe. Die Plattform ist sowohl für den Einsatz «On-Premise» als auch als Cloud-Lösung erhältlich.

Erfahrungen aus der Praxis zeigen, dass eine so konzipierte Isolationslösung Zero-Day-Angriffe und Drive-by-Attacken komplett unterbindet und für den Nutzer keine erkennbaren Einschränkungen oder Geschwindigkeitseinbussen mit sich bringt. Anwendungen mit über 100 000 Nutzern beweisen, dass das Konzept hervorragend auf grösste Umgebungen skaliert.



« Die Cybersicherheitstechnologie der Stunde nennt sich Browser-Isolation »

Roger Gomringer, Business Development Manager beim IT-Security-Distributor Boll Engineering, spricht im Interview über «Isolation» als neues Sicherheitskonzept, über die Marktentwicklung und die bisher ausgereifteste Implementation des wirksamen Prinzips. Interview: Oliver Schneider

Isolation ist ein vergleichsweise neues Konzept zur Steigerung der Cybersecurity. Wie entwickelt sich der Markt?
Roger Gomringer: Momentan ist der Markt noch überschaubar, wird sich aber stark entwickeln. So prognostiziert Gartner, dass im Jahr 2021 die Hälfte des Web-Traffics von Unternehmen isoliert ablaufen wird, und sieht Isolations- beziehungsweise Remote-Browser-Lösungen als Toptechnologie im Bereich Cybersecurity.

Entspricht Isolation tatsächlich einem Kundenwunsch oder ist das alles nur ein Hersteller-Hype?
Isolation ist ganz offensichtlich mehr als ein Hype und trifft den Nerv von Unternehmenskunden. Ein Beispiel dafür ist die amerikanische Bank JP Morgan Chase. Sie setzt auf die Menlo Security Isolation Platform, um riskante Websites zu entschärfen und Spear-Phishing über gefährliche Links in E-Mails zu bekämpfen.

Menlo Security verspricht 100 Prozent Malware-Freiheit. Wie ist das zu verstehen?
Webbasierte Angriffe wie Drive-by-Attacken werden durch die Menlo-Plattform zu 100 Prozent verhindert, da die Nutzer ausschliesslich ungefährliche, gerenderte Inhalte zu sehen bekommen – selbst die besten herkömmlichen Advanced-Threat-Protection-Lösungen können das nicht. Bei der Dokumenten-Isolation erstellt Menlo eine sichere Variante sämtlicher Dokumente. Diese sind frei von jeglichem aktiven Code und stehen dem User für den sicheren Download zur Verfügung. Ein Restrisiko bleibt dann vorhanden, wenn es das Unternehmen zulässt, dass dem User auch die Originalversion zur Verfügung steht. Vor diesem Hintergrund empfehlen wir ein ergänzendes Phishing- und Security-Awareness-Training für die Mitarbeitenden.

Was braucht es ausser der Menlo-Plattform noch, damit das Risiko weiter minimiert wird?
Der Web- und E-Mail-Isolation-Dienst kann zusammen mit herkömmlichen Sicherheitstechnologien wie Secure-Mail- und Web-Gateways eingesetzt werden und ergänzt diese um einen wichtigen Faktor: Der Angriffsvektor Drive-by-Attacke ist vollständig abgedeckt. Der Document-Isolation-Service lässt sich zudem optional mit einer Anti-Virus- und einer Sandbox-Komponente ergänzen, um die nötige Sicherheit beim Download der Originaldokumente zu gewährleisten.

Welche Kundensegmente sind besonders angesprochen?
Die Lösung ist ab 100 Nutzern sinnvoll einzusetzen. Grundsätzlich sprechen wir alle Organisationen beziehungsweise Firmen an, die den Mitarbeitenden grösstmögliche Freiheit im Internet bei höchstmöglicher Sicherheit bieten wollen. Die Kunden finden sich in Branchen wie Finance, Insurance, Industrie und Pharma sowie beim Bund.

Wie lässt sich Isolation in bestehende Infrastrukturen einbinden?
Die Menlo Security Isolation Platform funktioniert vom Netzwerk her gesehen als Proxy-Service und lässt sich sehr einfach ins Unternehmensnetz eingliedern. Als Cloud-Lösung kommt sie ohne Installation beim Kunden aus. Die On-Premise-Variante kann je nach Situation mit allen Komponenten in einer einzelnen virtuellen Maschine auf Basis von VMware ESXi oder in Multi-Node-Architektur implementiert werden.

Cloud versus On-Premise: Welche Variante ist in der Schweiz populärer?
Eindeutig die On-Premise-Variante. Für Kundensegmente wie Finanzdienstleister oder Pharma kommt die Weitergabe von Nutzerdaten in eine ausserhalb der Schweiz gehostete Cloud-Plattform nicht infrage. Die cloudbasierte Menlo-Plattform basiert auf Amazon Web Services, Standort für Schweizer Kunden ist die AWS-Region Frankfurt.