

Zapotrzebowanie rynku

- Większość użytkowników musi pamiętać od jednego do aż piętnastu różnych haseł, w zależności od liczby różnych aplikacji i usług, z których muszą korzystać.
- W miarę wzrostu liczby aplikacji i usług rośnie również liczba haseł do zapamiętania.
- Sytuacja, w której użytkownicy zapisują hasła, mając trudności z ich zapamiętaniem, powoduje obniżenie poziomu bezpieczeństwa.
- Personel pomocy technicznej jest regularnie bombardowany zgłoszeniami użytkowników, którzy zapomnieli swe hasła lub proszą o ich zresetowanie. W poniedziałki i dni poświęcone następuje prawdziwy zalew zgłoszeń związanych z zarządzaniem hasłami.
- Problem generuje koszty zarówno twarde, jak i miękkie, a także koszty wynikające ze związanych z nim zagrożeń bezpieczeństwa.
 - Zwykle długi czas oczekiwania użytkowników na zresetowanie haseł drastycznie obniża ich produktywność.
 - Do 35 procent wezwań pomocy technicznej to zgłoszenia związane z hasłami, a każde zresetowanie hasła może kosztować nawet 25 USD, co w przypadku firmy zatrudniającej 1000 pracowników przekłada się na koszt 141.650 USD w skali roku.
 - Koszty likwidacji skutków jednego włamania to średnio 6,6 mln USD, zaś niezachowanie zgodności z wymogami przepisów może za sobą pociągać kary i dodatkowe zagrożenia.
- Brak zarządzania hasłami za pomocą centralnego mechanizmu opartego na rolach lub politykach wprowadza zagrożenia bezpieczeństwa. Niemal połowa naruszeń bezpieczeństwa i ataków ma źródło wewnątrz firmy i powodowana jest przez aktualnych i byłych pracowników, którzy zachowują nieuprawniony dostęp do zasobów informatycznych.

Ocena szans sprzedaży

Obiecujący klient:

- Potrzebuje szybkiego efektu o natychmiast widocznej wartości
- Działa w branży wysoce uregulowanej przepisami, gdzie wymagane jest używanie haseł i audyty dostępu
- Działa w branży lub środowisku, w którym bezpieczeństwo ma wysoki priorytet, a ryzyko włamania jest niedopuszczalne
- Użytkownicy muszą codziennie korzystać z dziesięciu lub więcej aplikacji, usług lub zasobów
- Użytkownicy często współdzielą stacje robocze lub korzystają z wielu przestrzeni roboczych, w tym Internetu
- Firmy dysponujące istniejącą infrastrukturą zarządzania tożsamością i dostępem, taką jak Novell Identity Manager lub Novell Access Manager

Trudny klient:

- Użytkownicy korzystają codziennie jedynie z kilku aplikacji, usług lub zasobów i mogą bez trudu zapamiętać niezbędne hasła
- Firmy nie korzystające z Active Directory, Novell eDirectory lub katalogów zgodnych z LDAP v3

Możliwe korzyści

- Novell SecureLogin umożliwia użytkownikom dostęp do zasobów sieciowych z użyciem jednego loginu i hasła. Prosta i szybka instalacja zapewnia natychmiastowe, wyraźne korzyści:
- Po zalogowaniu się użytkownika do dowolnego komputera działającego w sieci, następuje automatyczne uwierzytelnienie dostępu do zgodnych z mechanizmem jednokrotnego logowania aplikacji, baz danych i platform systemowych, niezbędnych do produktywnego pracy – bez konieczności naciskania jakichkolwiek dodatkowych klawiszy.
 - Najlepszy w swojej klasie kreator sprawia, że integracja aplikacji z mechanizmem jednokrotnego logowania jest procesem prostym i zautomatyzowanym. Kreator SecureLogin współpracuje bez problemu z aplikacjami Windows i Java oraz aplikacjami internetowymi i korporacyjnymi. Automatycznie generuje niezbędne skrypty, zapewniając klientom i partnerom korzyści z jednokrotnego logowania o wiele szybciej, niż w przypadku innych rozwiązań.
 - Możliwość scentralizowanego administrowania pozwala informatykom łatwo zarządzać hasłami i politykami, przyznawać lub odbierać prawa dostępu oraz monitorować działania w ramach jednokrotnego logowania. SecureLogin współpracuje z szeregiem katalogów, wykorzystywanych do składowania tożsamości i haseł, w tym Active Directory, eDirectory i innymi katalogami zgodnymi z LDAP v3.
 - Wykorzystywany przez SecureLogin model bezpieczeństwa jest o wiele silniejszy, niż proste jednokrotne logowanie – SecureLogin przechwytuje i przechowuje nazwy użytkowników i hasła do każdego z udostępnionych zasobów, a następnie zarządza i automatyzuje dostęp użytkowników w oparciu o tożsamość, role i polityki.
 - W istocie zapewnia dodatkową warstwę ochrony, ponieważ użytkownicy nie muszą znać haseł, dających im dostęp do niewrażliwych zasobów; informatycy mogą ustawiać do tych zasobów bardzo mocne, skomplikowane hasła, których użytkownicy nawet nie zobaczą.
 - Jest to proste rozwiązanie, zapewniające bardzo duże oszczędności: przy 5.000 użytkowników, SecureLogin zapewnia zwrot inwestycji już po 10-ciu miesiącach. Oszczędności po kolejnym roku mogą sięgnąć nawet 440 tys. USD.
 - Gotowe do użycia mechanizmy raportowania pomagają udokumentować zgodność zarówno z wewnętrznymi politykami bezpieczeństwa, jak i z wymogami przepisów dotyczących dostępu.
 - Novell SecureLogin współpracuje z zaawansowanymi technologiami uwierzytelniania, w tym rozwiązaniami biometrycznymi i inteligentnymi kartami, zapewniając dodatkowe podwyższenie poziomu bezpieczeństwa. Jest również w stanie obsługiwać tysiące różnorodnych zastosowań i zasobów, w tym na platformach Windows i Linux.

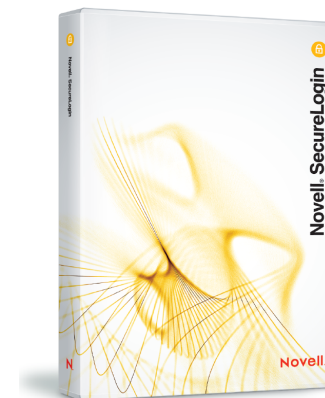
Pytania kwalifikacyjne

- Ile czasu zajmuje użytkownikom zalogowanie się do wielu różnych aplikacji, usług i zasobów, koniecznych im do wykonywania pracy?
- Jak wiele wezwań związanych z hasłami wpływa tygodniowo do działu pomocy technicznej?
- Jeśli każde takie wezwanie kosztuje firmę od 10 do 25 USD, jakie koszty generuje to w ciągu roku?
- Czy łatwo klientowi jest udokumentować zgodność z regulacjami dotyczącymi haseł, bezpieczeństwa i dostępu? Czy ma trudności z dostarczeniem wskaźników na potrzeby wewnętrznych audytów? Co będzie, jeśli te wskaźniki trzeba będzie udostępnić dla audytów zewnętrznych lub w związku z wymogami przepisów?
- Czy średnia moc używanych w firmie haseł jest zadowalająca? Czy klient chciałby egzekwować polityki silniejszych haseł? Co w tym przeszkadza?
- Czy wykorzystywane są współdzielone stacje robocze? Ile czasu zajmuje logowanie przy zmianie użytkowników?
- Czy klient jest zadowolony z bezpieczeństwa niewrażliwych aplikacji i zasobów? Czy bezpieczeństwo poprawiłoby się, gdyby użytkownicy nie musieli znać haseł do wszystkich systemów?

Ceny i licencjonowanie

Novell SecureLogin 7 – 41 euro za użytkownika z roczną priorytetową asystą techniczną

Novell SecureLogin zapewnia użytkownikom dostęp do zasobów sieciowych przy użyciu jednego loginu i hasła, automatycznie łącząc ich z użytkowymi przez nich aplikacjami. Dzięki temu, że użytkownicy muszą pamiętać tylko jeden login i hasło, firmy mogą praktycznie wyeliminować wezwania pomocy technicznej związane z hasłami, wymuszać stosowanie silnych haseł i egzekwować polityki związane z hasłami, a także zwiększyć produktywność użytkowników końcowych i personelu pomocy technicznej.



Konkurenci							Argumenty w dyskusji	
Cechy	CA	Citrix	Evidian	Imprivata	Passlogix	Novell SecureLogin	Wątpliwości	Odpowiedź
Kreator obsługuje aplikacje Windows i Java oraz aplikacje internetowe i korporacyjne	Nie	Nie	Nie	Tak	Tak	Tak	Już mam rozwiązanie do jednokrotnego logowania. Po co mi SecureLogin?	Po pierwsze, SecureLogin to o wiele więcej, niż tylko rozwiązanie do jednokrotnego logowania. Jest na tyle elastyczny, by kontrolować dostęp do systemów w oparciu o czas i adres URL, delegować dostęp do systemów, łączyć parametry logowania itd. Po drugie, zastosowane w SecureLogin podejście do jednokrotnego logowania zwiększa bezpieczeństwo w sposób niedostępny przy użyciu innych rozwiązań do jednokrotnego logowania, ze scentralizowanym, opartym na politykach zarządzaniem, zapewniającym informatykom precyzyjną, natychmiastową kontrolę nad dostępem.
Ścisła integracja z własnymi technologiami tożsamości i bezpieczeństwa	Nie	Nie	Nie	Nie	Nie	Tak	W jaki sposób SecureLogin zwiększa bezpieczeństwo systemu haseł?	Novell SecureLogin pozwala użytkownikom zarządzać wieloma hasłami. Dzięki temu użytkownicy nie tylko nie muszą pamiętać wielu haseł, ale zwykle nawet nie muszą ich znać. Za pomocą SecureLogin informatycy mogą tworzyć wysoce złożone hasła dla wewnętrznych i niewrażliwych aplikacji, przypisując je nie tyle do użytkowników, co do ich tożsamości, co zapewnia dodatkową, drugą warstwę zabezpieczeń. Ponieważ haseł nie trzeba pamiętać, mogą one być bardzo skomplikowane, na tyle mocne, by spełniać najwyższe standardy bezpieczeństwa. Ponadto użytkownicy nie muszą znać – a nawet kiedykolwiek widzieć – haseł do niewrażliwych aplikacji, do których mają dostęp. Muszą pamiętać tylko jeden login i hasło, a SecureLogin zarządza pozostałymi hasłami, zapewniając w niewidoczny sposób bezproblemowy i bezpieczny dostęp do zasobów.
Gotowość do pracy z Active Directory, eDirectory i katalogami zgodnymi z LDAP v3	Nie	Nie	Nie	Nie	Nie	Tak	Ale ja używam Windows. Nie chcę wprowadzać do mojej infrastruktury rozwiązania, które będzie trudne do wdrożenia i zintegrowania.	Novell SecureLogin współpracuje z Windows. Co więcej, jest łatwy do wdrożenia, jest fabrycznie przygotowany do pracy z tysiącami aplikacji (nie jest konieczne programowanie ani ręczne konfigurowanie) i bez problemów integruje się z popularnymi katalogami, platformami i przeglądarkami internetowymi, w tym obecnymi w kręgach Windows, Linux, Citrix czy LDAP. Prosty proces instalacji pozwala wdrożyć jednokrotne logowanie w mieszanej infrastrukturze w ciągu dni, a nie tygodni czy miesięcy. Nie jest konieczna przebudowa środowiska informatycznego. To rozwiązanie zapewniające natychmiastowe korzyści.
Niszowy gracz w dziedzinie jednokrotnego logowania	Nie	Tak	Tak	Tak	Tak	Nie		
Koszt	\$\$	\$\$	\$\$	\$\$\$	\$\$	\$		

Szkielet rozwiązania

Atuty rynkowe

- Zgodność z wymogami przepisów dotyczących haseł i kontroli dostępu
- Egzekwowalne polityki i standardy haseł o określonej mocy
- Zwiększenie produktywności użytkowników przy jednoczesnym obniżeniu kosztów informatyki

Typowy klient

- Wysoki priorytet bezpieczeństwa, zwłaszcza w odniesieniu do niewrażliwych aplikacji
- Regularne audyty zgodności z wymogami dotyczącymi haseł i dostępu
- Użytkownicy korzystają codziennie z dziesięciu lub więcej aplikacji

Rozwiązanie

- Novell SecureLogin jako fundament mechanizmu jednokrotnego logowania, chroniący dostęp do niewrażliwych aplikacji poprzez oparte na tożsamości zarządzanie i egzekwowanie wysoce złożonych standardów polityk haseł.
- Dodatkowe możliwości sprzedaży obejmują Novell Identity Manager i Novell Access Manager, których dodanie pozwala stworzyć ściśle zintegrowane, całościowe rozwiązanie zarządzania tożsamością i bezpieczeństwem.

