In today’s connected world, outsider threats are real and—at times—daunting. User credentials for access serve as an essential layer of defence. As such, advanced authentication is too important of a component of your security strategy to patch together as siloed or even disparate infrastructures across your organisation. In this white paper, you will find out how Micro Focus® Advanced Authentication can enable secure interaction with employees, partners, and customers.
Risk and Mobility
Make Username/Password Untenable

Whether organisations are seeking to protect themselves from outsiders or simply comply with government mandates, user verification continues to be a cat and mouse game between security and risk. Organisations do what they must to manage their risk while outsiders evolve their attack methods as they look for weaknesses and vulnerabilities. Today, hackers target primarily private information like intellectual property, patient records, credit card or bank account information.

For organisations who view their risks as minimal and do not see advanced authentication technology as a business enabler, they are more likely to rely on out-of-date credential management practices. This lag-gard approach is especially common for those who have not suffered a major incident. Interestingly, SMB’s often view their risk as low because of their relatively small size. In fact, according to a survey conducted by Manta, an SMB services company, 97% of SMBs surveyed do not believe they are at risk for a breach even though half of them experience some level of intrusion each year.

Figure 1. In a survey by Manta, an SMB services company, 97% of SMBs surveyed do not believe they are at risk for a breach even though half of them experience some level of intrusion each year.
Although many organisations view user verification as an afterthought, it is important to note that according to Verizon’s latest DBIR report, over 80% of hacking-related breaches studied succeeded by leveraging either stolen passwords or by ones that were weak or guessable. Which means that for many organisations it is simply a matter of time before they suffer an event where they lose sensitive information that results in a tangible financial loss, not to mention loss of customer trust.

What makes these trends notable is that there has never been a time when advanced authentication is as convenient and affordable to implement as it is today. Traditionally, organisations have been limiting their multi-factor authentication implementations to a small subset of specialised users who work with information that poses a higher level of risk to the business. Cost and usability have often been the limiting factors preventing wider deployments of strong authentication technology. Historically, strong authentication methods were expensive to purchase, deploy (including enrolling the users), and administer. But recently, there has been a sweeping set of changes across multiple industries, within the organisations themselves, their customers (or patients, citizens, partners, etc.), and the technology that they have access to.

“Advanced authentication has never been as convenient and affordable to implement as it is today.”

Figure 2. Verizon 2017 Data Breach Investigations Report.
The main business drivers changing authentication include:

- Most industries must comply with some type of privacy law concerning customer, patient, or financial information. In addition, government agencies continue to firm up their policies requiring multi-factor authentication for user identity verification.

- Today, more than ever, professionals are doing work outside the office, either as road warriors or as remote employees. These users are accessing information of all levels of sensitivities (customer, patient, citizen, HR, etc.), which are subject to specific multi-factor authentication government mandates.

- People and the organisations they interact with do so in the context of a pervasively connected world. The old days of accessing information through dedicated lines or in confined corporate intranets are long gone. Today, privileged insiders, and their devices, are sharing the same internet with the masses.

- Virtually everyone has a connected computer (smartphone) in their pocket from which they conduct their lives: social media, consumer personalised content, and e-commerce. Because customers expect to interact with businesses digitally on their devices, organisations that are not aggressively pursuing the ultimate digital experience for their customers (patients, citizens, etc.) will find themselves irrelevant. The reality is that mobile devices are today’s tier one platform, which elevates the importance of providing connectivity and content on those form factors.

It is in this context of digital interaction that we read about the continual stream of breach notices where private information is exposed in just about every type of institution: corporate enterprise, SMB, federal, state and local, health care, financial services, retail, political, entertainment, etc. All of which forces these organisations to up their security game while wrestling with maintaining or increasing the ever-important user convenience.
Think Strategic (Long Term), Not Tactical (Today’s Project)

As your organisation evolves its authentication capabilities beyond user names and passwords, you have several important determinations to make. These decisions could affect your level of security, overhead of administration, and even the level of convenience that you are able to offer your users. The key point is that these authentication virtues will often come down to how much flexibility you have to adopt the right authentication type and method. Ultimately, you need to decide how important it is to have the freedom to use the latest strong authentication technology at the best price.

You also need to decide how important it is to have a single point of integration for your entire environment: all your employees at all your sites, partners, customers, etc. Having multiple authentication infrastructures silos the administration of policies, which not only increases overhead but is also the source of uneven policies and security. It is often the out-of-date profile of a long-departed user whose identity is still active that poses a risk or a user whose authentication profile is too weak for the risk they pose to the firm.

Below are some real world advantages you get with Advanced Authentication:

- **Open Architecture for Integration**
  
  Did you know that you can centralise all your authentication into a single framework? We use open standards, so you have a foundation to build on without the fear of being locked in. And because of our broad set of integrations and aggressive support, you will have the freedom to use the appliances that best fit your needs.

  Organisations are usually forced to manage and maintain multiple infrastructures. Not only are multiple authentication infrastructures complicated to manage, but they are also less secure. What you need is a single authentication framework for all of your devices and methods. Having a single framework keeps costs down as Advanced Authentication scales to any size environment.

  Because it takes a standards-based approach to application integration, Advanced Authentication provides an OAuth interface that provides clients an easy way to integrate their applications. Once in place, applications can leverage Advanced Authentication’s policy engine to match the appropriate method(s) to the situation to provide the ‘right’ level of security.
Centralised Policy Engine
The Advanced Authentication framework is robust enough to manage large environments with diverse authentication needs but simple enough to require little administration. With our two-factor (or more) authentication capabilities, you can create authentication policies specific to users, groups, devices, or locations. The web interface keeps configuration clean, regardless of complexity. Delegated administration and tracking of changes keeps policies consistent and secure. And because the policy engine in the Advanced Authentication framework is flexible, it crosses all authentication methods, alleviating redundant work and inconsistent authentication.

Universal Client Support
Advanced Authentication adapts to your needs by giving you the broadest platform coverage available. It supports Windows, OS X, and Linux operating systems.

U2F Ready
Micro Focus is a member and strong supporter of FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) provides a way for organisations to support an environment where users manage their own authentication devices. Advanced Authentication provides a solid framework to deliver that support to your applications without the need for development. Organisations benefit from deferring token costs, and users like them because they are able to incorporate a higher level of security across other aspects of their digital life. Advanced Authentication delivers broad application support as well as a lower total cost of ownership. There is no better framework from which to provide a U2F authentication environment.

Web-Based Administration, Configuration, and Enrolment
Because the administrative and configuration operations are web-based, you can perform all of your administrative needs in one console using any device with a browser. Advanced Authentication provides an easy, self-explanatory workflow for the end user registration experience. By simplifying the registration of iOS, Android, and Windows Phone devices; workstation connected biometrics; card readers; and others, your users will effectively register their devices, your system will easily scale, and your helpdesk will not be overrun with registration issue calls.

BYOD Support
In a day and age where employees and contractors are using their own devices (BYOD), it is likely that they are not part of your corporate domain. Because Advanced Authentication does not require domain membership, multi-factor authentication is not limited to just your corporate devices. Your users can bring their Windows, Mac OS X, and even Linux-based systems, and you can enforce Advanced Authentication to your resources as needed.
Simplifying the Time-Consuming Tasks of Advanced Authentication

The helpdesk module provides the capabilities to ensure a good end-to-end customer experience. These capabilities include un-enrolling and assisting in re-enrolling methods, assigning tokens (when needed), and assigning specific user roles. If a user contacts the helpdesk with an authentication issue related to Advanced Authentication, your helpdesk agent will be able to provide the positive customer support experience expected. This builds strong relationships and further support for your multi-factor authentication efforts.

Use this Advanced Authentication feature when a user has no previously enroled authentication method available. Perhaps your user misplaced their token, took their phone swimming, or they could just be at a workstation where the card reader has failed. In any event, they still need access. The Emergency one-time password (OTP) access process is part of the helpdesk module and allows for an OTP to be generated for the user in these urgent situations.

Support for Road Warriors

Think of situations where professionals are out in the field accessing private information while on the road. Inevitably, users on the road will occasionally be unable to connect. But many organisations still expect work to continue. For example, one of our customers is a power company that has field workers who need access to sensitive power grid information and schematics: transmission grids, distribution grids, transition stations, substations, etc. While access security was a must, reliable access in all situations was also critical.

Scales Up and Out

Large or distributed organisations will benefit greatly from a single set of worldwide authentication policies. Advanced Authentication supports multi-site configurations that are designed to scale to virtually any performance or location requirement. It can also be configured to deliver regional clusters for high availability, providing continuous, uninterrupted operations.

Application availability, reliability, and performance are assured with internal server load balancing capabilities. Multiple updated data stores are always available for rapid disaster recovery (DR), while replication between primary and secondary locations (over LAN or WAN) ensures data integrity.

Strong Authentication ADFS

You can configure Active Directory Federation Services (ADFS) to use our flexible Advanced Authentication framework. If your organisation uses any ADFS services that serve applications that need multi-factor authentication or other types of strong authentication protection, there is a good chance that you will more than just a mobile OTP, which is all that it allows. Advanced Authentication can also be configured across multiple Microsoft Azure configurations. And because Advanced Authentication integrates natively into ADFS, you have the flexibility to use any authentication type that you like to protect the services federated with it.
The Best Strong Authentication Solution

What makes Advanced Authentication different? Our open architecture approach and focus on giving you the widest range of authentication method options, the broadest coverage of platforms and applications. We do not participate in business partnerships that limit your choice of methods, rather, we aggressively pursue expanding the number of strong authentication options that you have as soon as possible.

The soft appliance is designed to be quick to set-up with minimal maintenance. And yet, it is simple to scale up to the most demanding environments or grow outward to fill worldwide distributed ones. Regardless of the layout of your corporate environment, Advanced Authentication offers a single pane of glass control of all your authentication policies and users. For those that do not wish to deploy and manage Advanced Authentication on your own, it is available in its complete form in the cloud as a service; meaning that the cloud based authentication is equal in functionality to the on-prem edition.

Learn More At
http://smbsoup.com/2016/10/small-business-cybersecurity-large-holes-study-finds/
www.esecurityplanet.com/network-security/50-percent-of-smbs-were-breached-in-the-past-year.html