THREATMETRIX:
PIONEERING CONTEXT-BASED WORKFORCE AUTHENTICATION

Reed Taussig,
President & CEO,
ThreatMetrix
The consumerization of IT is well underway. The network perimeter has virtually disappeared, a modern workforce connects from inside and outside of the corporate firewall to both on-premise and cloud-hosted applications. As BYOD is now a business reality, corporate IT has lost visibility and control over the devices that employees and contractors use to access both critical and non-critical applications.

In this fast-changing IT environment, traditional access security controls are increasingly archaic and unworkable. Today employees accessing mission-critical applications look like consumers on ecommerce websites. Enterprise security practitioners must find new approaches for securing access to corporate applications to address a major source of risk.

ThreatMetrix™ is helping businesses apply techniques of context-based authentication and federated trust to address the growing problem of remote workforce authentication. Gartner estimates that by year end 2016, more than 30 percent of enterprises will use contextual authentication for remote workforce remote access. [Source: Gartner Magic Quadrant for User Authentication, December, 2013]

The Challenge of Remote Workforce Access
Remote workforce logins are open to the same types of misuse and abuse as consumer-based applications with potentially far greater business risk. A cybercriminal logging into an employee’s account using stolen credentials can do far greater damage to a company than a customer using a stolen credit card.

“Endpoint trustworthiness is especially poignant for bring-your-own-device (BYOD) scenarios. In such cases, the enterprise may not use mobile device management (MDM) software to help secure workforce mobile devices. As a result, employee phones and tablets may look very much like consumer devices, and it’s important to decide how much to trust the user and the credentials and the contextual information that they’re presenting.” [Source: “Adaptive Access Control Brings Together Identity, Risk and Context,” Gartner: Trent Henry, August 2013]

Enterprise security professionals must walk a fine line when it comes to securing workforce access to applications. On the one hand, mitigating the risks of data breaches is a top priority – no company wants to end up on the front page of The Wall Street Journal as a high profile data breach.

On the other hand, security must be balanced with the user experience. Time-consuming authentication techniques erode overall productivity. Worse, the more onerous the security measures, the more motivated the workforce will be to find ways around them.

Traditionally, companies lock down remote logins by deploying VPNs, requiring employees and partners to use corporate-issued equipment, or issuing hardware tokens or one-time passwords (OTP) for strong authentication. These methods are getting more and more impracticable in today’s “consumerized” IT environment.

Context-Based Authentication and Federated Trust
ThreatMetrix offers an alternative to traditional workforce authentication models, leveraging a shared trust intelligence network that currently protects more than 2,500 financial services and e-commerce companies from global cybercriminal rings.

ThreatMetrix offers real-time technologies that analyze online personas, employee devices, transactional or application context and employee behavior. As a passive, network-based solution delivered from the cloud, ThreatMetrix is capable of recognizing all employee-supplied devices, whether they have authenticated in the past or not. A global policy engine lets...
businesses define specific and appropriate risk and access policies. Using ThreatMetrix, businesses can tag trusted combinations of credentials and identify indicators of risk learned from a global network of online identities, transactions and data.

By analyzing the contextual information from the login and comparing it to data from a global network, ThreatMetrix can help businesses reduce the risk of remote login without burdening the user.

“Enterprise adaptive access control combines contextual information and user credentials to reduce the risk of users attempting to access resources. Once the purview of e-commerce and financial services, adaptive access is finding an increased role in workforce identity — particularly for mobile device use cases.”

-Gartner: Trent Henry, August 2013

“Together Identity, Risk and Context,” particularly for mobile device use cases.”

ThreatMetrix can help businesses reduce the risk of remote login without burdening the user.

“Context-based authentication has two essential benefits for the enterprise:

• Frictionless access: Real-time, passive authentication of the login context gives businesses the ability to streamline access for known and trusted combinations of logins and devices — reducing effort and inconvenience for the workforce.

• Increased security: Combining global federated trusted identities with context-based authentication helps businesses quickly and easily identify high-risk connections that have the potential to compromise data. This includes devices that are part of botnets, devices associated with many different unregistered credentials that are used to create a cloud of identity or devices that are known to be involved with fraudulent access across the ThreatMetrix global network.

The Frictionless Login

A typical implementation works like this:

1. The first time an employee logs into a sensitive application such as a financial system, ThreatMetrix creates a profile of the incoming user. The individual is prompted to perform step-up authentication, perhaps using an OTP sent to their registered mobile phone. At this point, ThreatMetrix tags that trusted combination of device and account for future reference.

2. The next time that employee logs in, the ThreatMetrix platform does a real-time analysis for any threats (malware, etc.) and identifies the trusted online identity. This is transparent to the employee.

3. If the employee gets a new laptop or tablet and that device has been authenticated with appropriate and acceptable credentials anywhere across the ThreatMetrix network, the enterprise can choose how to address the situation: accept those credentials without challenge or execute a challenge to further authenticate that user’s credentials.

Every transaction is screened for other indicators of risk, including malware, bots and behavioral risk factors.

4. Combining real-time contextual authentication with federated trusted identity data derived from the ThreatMetrix network provides seamless, reliable identification of user credentials without the need to install and maintain MDM, token or other device-specific solutions.

Using this process, businesses can detect anomalies and keep hackers out while streamlining legitimate workforce connections. It can also detect anomalous behavior, detect an insider threat, such as unauthorized password sharing that puts regulatory compliance at risk.

Benefitting from the Network Effect

The power of the ThreatMetrix solution comes not only from its technologies, but also from the data it collects and analyzes across its global network.

The forces arrayed against the enterprise are growing in size and sophistication. A few years ago most data breach attempts came from clumsy phishing emails and opportunistic, individual hackers. Today’s online threat environment is characterized by well-organized and well-financed cyber-terrorist rings and crowd-sourced malware and botnets. The only viable defense against these global forces is a global network.

From its inception in 2005, ThreatMetrix has been developing a global network in the fight against cybercrime. Supporting over 2,500 of the world’s largest Internet retailers, financial institutions and social networking sites, ThreatMetrix has built a federated trust network that examines tens of millions of employee and customer logins and account registrations every day. Using the power of shared intelligence across more than 10,000 customer websites ThreatMetrix provides the largest federated trust network in the world.

All of the devices, persona and transactions that take place across the customers’ websites in the ThreatMetrix network are shared as part of the ThreatMetrix™ Global Trust Intelligence Network (The Network). Data on The Network includes device identification characteristics, user and persona profiles, behavior, detected relationships and threat assessments. This massive data set is refreshed and analyzed continuously to identify emerging threats.

All ThreatMetrix customers contribute value by sharing anonymous data with the Network. In turn, all participants of the Network benefit from the global threat intelligence developed by the network. To protect user privacy, all of a business’ data is encrypted and anonymized before being sent to the global network. Within the ThreatMetrix platform, multi-level encryption ensures that data remains private between all the participants in the network, including ThreatMetrix.

“It is the power of The Network that provides our customers with this world-class and cost-effective solution,” says Reed Taussig, President and CEO of ThreatMetrix. “Rather than deriving decision data from a single enterprise, ThreatMetrix customers share anonymous data globally. This increases the perspective, quality and value of the data while driving down the cost to the enterprise.”

Extending the Power of the Network

With hundreds of millions of transactions available each month, ThreatMetrix is using “big data” techniques to mine this information for insight that benefits all of its customers, as well as the Internet as a whole. One can see the real-time analysis of fraud attempts detected throughout the global network on the ThreatMetrix Web Fraud Map.

For businesses looking to reduce the threat of data breaches from unauthorized access, combining context-based authentication with a global federated identity network is the most flexible and cost-effective way to increase security while reducing the cost and friction for workforce access.